On Dihedral Representations Arising From Modular Elliptic Curves

Imin Chen
chen@math.mcgill.ca
http://www.math.mcgill.ca/~chen

24 June 1999

Let $\overline{\rho}_\ell : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_\ell)$ be the mod ℓ representation attached to an elliptic curve $E/\mathbb{Q}$.

Let $S_{E/\mathbb{Q}}$ be the set of all primes ℓ for which $\overline{\rho}_\ell$ is not surjective.

Theorem 1 (Serre) *If $E/\mathbb{Q}$ does not have complex multiplication, then $S_{E/\mathbb{Q}}$ is finite.*

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication throughout.

If $\overline{\rho}_\ell$ is not surjective, then its image lies in
1. a subgroup whose projective image is S_4
2. a Borel subgroup
3. the normalizer of a Cartan subgroup but not in a Cartan subgroup

Case 1 can only occur if $\ell \leq 13$ by a calculation of Serre.

Case 2 can only occur if $\ell \leq 37$ by Mazur's bound on rational torsion subgroups.

Case 3 is the problematic one. Such mod ℓ representations have projective image a dihedral group D_ℓ. We say $\overline{\rho}_\ell$ is split or non-split dihedral according to whether its image lies in the normalizer of a split or non-split Cartan subgroup.

Let $D_{E/\mathbb{Q}}$, $D^+_{E/\mathbb{Q}}$, $D^-_{E/\mathbb{Q}}$ denote the set of primes ℓ for which $\overline{\rho}_\ell$ is dihedral, split dihedral, non-split dihedral, respectively.

The set $D_{E/\mathbb{Q}}$ is related to congruence primes (c.f. Ribet). This can be seen as follows.

Suppose now that $E/\mathbb{Q}$ is a modular elliptic curve without complex multiplication.

Attached to $E/\mathbb{Q}$ is a newform $f \in S_2(\Gamma_0(N))$ of level N equal to the conductor of $E/\mathbb{Q}$.

Let $\ell \in D_{E/\mathbb{Q}}$ be such that $\overline{\rho}_\ell$ is dihedral. Attached to $\overline{\rho}_\ell$ is a quadratic field $K/\mathbb{Q}$ corresponding to the character

$$\overline{\epsilon} : G_{\mathbb{Q}} \xrightarrow{\overline{\rho}} GL_2(\mathbb{F}_\ell) \to PGL_2(\mathbb{F}_\ell) \to D_\ell/C_\ell = \{\pm 1\}$$

C_ℓ is the cyclic group associated to the dihedral group D_ℓ.

The quadratic field K is imaginary when $\ell \in D^-_{E/\mathbb{Q}}$ since $\overline{\rho}(c)$ has characteristic polynomial $X^2 - 1$ as $\overline{\rho}$ is odd, but there are no such elements in C_ℓ.

If $\ell > 3$ and $\ell \nmid N$, then one can show that the twist g of f by $\overline{\epsilon}$ is also a newform $g \in S_2(\Gamma_0(N))$ which is congruent modulo ℓ to f. So ℓ is a congruence prime for $f \in S_2(\Gamma_0(N))$ in the sense that $a_n(g) \equiv a_n(f) \pmod{\ell}$ for all $(n, N) = 1$.

Bounds for such congruence primes show that $\ell < C = 68N'(1 + \log\log N')^{1/2}$, where $N' = \prod_{p|N} p$.

Theorem 2 (Kraus) *If $E/\mathbb{Q}$ is modular, then $\ell \in D_{E/\mathbb{Q}}$ satisfies $\ell < C$.*

The above is essentially the proof of Kraus that the primes in $D_{E/\mathbb{Q}}$ are $< C$ for a modular elliptic curve, but we have interpreted his proof in terms of congruence primes.

It has been shown that if $27 \nmid N$, then $E/\mathbb{Q}$ is modular. Problems occur when $27 \mid N$ because one uses $\overline{\rho}_3$ to prove $E/\mathbb{Q}$ is modular, and 3 is still to small to behave well.

We remark: if $\overline{\rho}_\ell$ is dihedral for $\ell > 3$ and $\ell \nmid N$, one can apply Diamond's generalization of Wiles' lifting criterion to $\overline{\rho}_\ell$ instead to show such an $E/\mathbb{Q}$ is already modular.

Theorem 3 *Kraus' bound is unconditional. That is, $\ell \in D_{E/\mathbb{Q}}$ satisfies $\ell < C = 68N'(1+\log\log N')^{1/2}$ for any elliptic curve $E/\mathbb{Q}$.*

We would like to discuss a different way to see the connection of $D_{E/\mathbb{Q}}$ to congruence primes, in particular $D^-_{E/\mathbb{Q}}$.

Theorem 4 *If $\ell \in D^-_{E/\mathbb{Q}}$, $\ell > 3$ and $\ell \nmid N$, then there exists a normalized eigenform $g \in S_2(\Gamma_0(N))$ which is congruent modulo ℓ to f, and is induced from a grossencharacter on an imaginary quadratic field.*

The imaginary quadratic field in question is just K.

This phenomenon can be seen in the work of Momose who showed the special case when N is a prime power under certain technical hypotheses, and Chapter 4 of Wiles when he shows lifts of split dihedral representations are modular when K is imaginary quadratic.

A quick example from Cremona's tables: 4176N

$E/\mathbb{Q} : y^2 = x^3 - 3105x + 139239$

$N = 4176 = 2^4 3^2 29$

$\Delta = -2^4 3^9 29^5$

$j = -10512288000/20511149 = 2^8 3^3 5^3 23^3/29^5$
$= 125\frac{t(2t+1)^3(2t^2+7t+8)^3}{(t^2+t-1)^5}$ for $t = -4/5$ so $\overline{\rho}_\ell$ is non-split dihedral.

This follows from the fact that there is a modular curve $X_{ns}(5)/\mathbb{Q}$ whose $\mathbb{Q}$-points correspond to elliptic curves $E/\mathbb{Q}$ whose $\overline{\rho}_5$ is non-split dihedral. There is a natural covering map

$$X_{ns}(5)/\mathbb{Q} \to X(1)/\mathbb{Q}.$$

It turns out that $X_{ns}(5)/\mathbb{Q}$ is isomorphic to $\mathbb{P}^1/\mathbb{Q}$, and if we let $t/\mathbb{Q}$ be a suitably chosen uniformizer, the covering map is given by the above relation between $j/\mathbb{Q}$ and $t/\mathbb{Q}$.

Since $E/\mathbb{Q}$ is semi-stable at 29, and the exponent of 29 in Δ is divisible by 5, by Ribet's theorem, $\overline{\rho}_\ell$ is modular of level $144 = 2^4 3^2$.

Indeed, there is a newform g at level 144 which is congruent modulo 5 to f.

$a_p(g) = [-, +, 0, 4, 0, 2, 0, -8, 0, 0, 4, -10, 0, -8, 0, 0,$

$a_p(f) = [-, +, 0, -1, -5, -3, 5, 2, 0, +, -6, 10, 10, 2,$

The newform g corresponds to the isogeny class of elliptic curves 144A which have complex multiplication by $\sqrt{-3}$, so g is induced from a grossencharacter on an imaginary quadratic field.

Idea of the proof of Theorem 4.

Suppose $\overline{\rho} = \overline{\rho}_\ell$ is non-split dihedral. It is then induced from a one-dimensional mod ℓ representation $\overline{\chi}$ of G_K: $\overline{\rho} \cong Ind_K^{\mathbb{Q}} \overline{\chi}$. The quadratic field K is imaginary in this case, and $\overline{\chi}$ is defined over $\mathbb{F}_{\ell^2-1}$.

Composing $\overline{\chi}$ with the Teichmüller lift $\mathbb{F}_{\ell^2-1}^\times \to \widetilde{L}^\times \to \widetilde{L}_\lambda^\times$ we obtain a one-dimensional λ-adic representation $\widetilde{\chi}$, where $\widetilde{L} = \mathbb{Q}(\zeta_{\ell^2-1})$, and λ is a prime of $\widetilde{L}$ above ℓ.

We now use some results from Serre's theory of abelian λ-adic representations.

Serre showed that there is an algebraic group $S_\mathfrak{m}$ defined over $\mathbb{Q}$ for any modulus $\mathfrak{m}$ of K from which any algebraic representation $\phi : S_\mathfrak{m}/L \to GL_n/L$ defined over a number field L gives rise to a strictly compatible system of λ-adic representations $\chi_\lambda : G_K \to GL_n(L_\lambda)$ which are

1. abelian
2. semi-simple
3. locally algebraic
4. have conductor dividing $\mathfrak{m}$
5. L-rational

where λ is a prime of L above ℓ.

Locally algebraic is a technical term which says that the restriction of these λ-adic representations to inertia groups at ℓ are in some sense given by algebraic homomorphisms.

This is the analogue for GL_1 of some of the restrictions Wiles' places on his (non-abelian) two-dimensional λ-adic representations. However, the picture in the abelian case is pretty complete because we have class field theory, unlike the case of GL_2.

The conductor is a modulus of $\mathfrak{m}$ which measures the ramification of a λ-adic representations at both places $v \nmid \ell$ and $v \mid \ell$. For the latter to make sense, one requires the hypotheses of locally algebraic.

For convenience, we say an abelian λ-adic representation has level $\mathfrak{m}$ if its conductor divides $\mathfrak{m}$.

L-rational means that the characteristic polynomials of Frobenius conjugacy classes at unramified places have coefficients in L.

For $\phi : S_{\mathfrak{m}}/L \to GL_1/L$ one-dimensional, one might like to think of ϕ as an eigenform on GL_1/K, and the above as analogue of Deligne's theorem for GL_1 over a number field.

$S_{\mathfrak{m}}/\mathbb{Q}$ is roughly the product of $T = Res_K^{\mathbb{Q}}(\mathbb{G}_m/K)$ and the ray class group $C_{\mathfrak{m}}$ of modulus $\mathfrak{m}$, with some twisted galois action. It satisfies an exact sequence:

$$1 \to T_{\mathfrak{m}} \to S_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1$$

where $T_{\mathfrak{m}}$ is the quotient of T by the Zariski closure of the units $\equiv 1 \pmod{\mathfrak{m}}$ in $K^\times = T(\mathbb{Q})$.

Serre showed that any abelian λ-adic representation χ which is L-rational and semi-simple arises from such an algebraic representation $\phi : S_{\mathfrak{m}}/L \to GL_n/L$, with $\mathfrak{m}$ being the conductor of χ.

At least he did this for $K/\mathbb{Q}$ quadratic and $L = \mathbb{Q}$. The general case is due to Henniart.

Our $\widetilde{\chi}$ is $\widetilde{L}$-rational, and it can be shown that it has level $\mathfrak{m}\ell$ (i.e. conductor dividing $\mathfrak{m}\ell$), where

$\mathfrak{m}$ is the Artin conductor of the mod ℓ representation $\overline{\chi}$.

So our $\widetilde{\chi}$ arises from an algebraic character $\phi : S_{\mathfrak{m}\ell}/\widetilde{L} \to GL_1/\widetilde{L}$. As ϕ is in some sense an modular form for GL_1, it has an associated weight $k \in \mathbb{Z}[J]$ where $J = \left\{\sigma : K \to \overline{\mathbb{Q}}\right\} = \{1, \tau\}$. This is obtained by restricting ϕ to $T \to T_{\mathfrak{m}} \to S_{\mathfrak{m}}$ to get an algebraic character $\phi\,|_T$: $T/L \to GL_1/L$. A calculation shows that $\widetilde{\chi}$ has weight 0.

We say that $\overline{\chi}$ is modular of type $(0, \mathfrak{m}\ell)$ as it is the reduction of a λ-adic representation $\widetilde{\chi}$ of weight 0 and level $\mathfrak{m}\ell$.

In analogy with the refined Serre's conjectures for two-dimensional mod ℓ representations, one can define an optimal weight and level for which $\overline{\chi}$ is modular. In the situation at hand, the optimal weight is 1, and the optimal level is the Artin conductor $\mathfrak{m}$ of $\overline{\chi}$.

Using the fact that $\overline{\chi}$ is modular of type $(0, \mathfrak{m}\ell)$ we show that it is modular of type $(1, \mathfrak{m})$ at the optimal weight and level.

Thus, there is a $\phi : S_{\mathfrak{m}}/L \to GL_1/L$ such that its associated χ_λ reduces modulo λ to $\overline{\chi}$.

Now, associated to ϕ is also a grossencharacter χ_∞ of weight 1 and modulus $\mathfrak{m}$ in the usual sense. This is the archimedean analogue of the construction of the χ_λ's from ϕ.

Let g be the normalized eigenform attached to χ_∞ via Hecke. It has level $M = |d_K| \, N_{K/\mathbb{Q}}(\mathfrak{m})$, weight 2, and satisfies the property that its fourier coefficients lie in L, and its associated λ-adic representations satisfy $\rho_{g,\lambda} \cong Ind_K^{\mathbb{Q}} \chi_\lambda$.

Because $\ell > 3$ and $\ell \nmid N$, one can show that K is unramified at ℓ. We then have that the Artin conductor of $\overline{\rho} \cong Ind_K^{\mathbb{Q}} \overline{\chi}$ is $|d_K|\, N_{K/\mathbb{Q}}(\mathfrak{m}) = M$, and thus $M \mid N$.

By construction, $\overline{\rho}_{g,\lambda} \cong Ind_K^{\mathbb{Q}} \overline{\chi} \cong \overline{\rho}_{f,\lambda}$, so g is congruent to f modulo ℓ.

However, $g \in S_2(\Gamma_1(M))$ so far and may have non-trivial character ψ. A lemma analogous to Carayol's lemma for $GL_2/\mathbb{Q}$ shows that we could have chosen ϕ so the corresponding g has trivial character.

Recall Carayol's lemma for $GL_2/\mathbb{Q}$ (true for $\ell > 3$) roughly says that if $\overline{\rho}$ is modular of character ψ, and $\psi' \equiv \psi \pmod{\lambda}$, then $\overline{\rho}$ is also modular of character ψ'.

One can check that the character ψ of g is congruent to 1 modulo λ, so Carayol's lemma says it is also modular of trivial character.

It can be checked that the property of $\overline{\rho}$ arising from a normalized eigenform induced from a grossencharacter is still preserved when going from character ψ to the trivial character.

Some further examples, where some of the hypotheses are not satisfied. In addition to Cremona's tables, we use some tables of modular forms computed by William Stein.

675B:

$E : y^2 + xy + y = x^3 - x^2 - 5x + 2$

$N = 3^3 5^2$

$j = 1875 = 35^4, t = -3$ so $\overline{\rho}_5$ is non-split dihedral.

$\Delta = 6075 = 3^5 5^2$

There is a newform g (E[675,3] in Stein's tables) given by

$a_p(g) = [x, 0, 0, 0, 0, 0, -2x + 9, -6x + 7, -4x + 9, 0, 6x - 13, 0, 0, 0, -8x + 12, 2x + 9, 0, -12x + 17,$

$a_p(f) = [-1, +, +, 0, -5, 5, -4, -2, 3, -10, 6, -5, -10, -10, 5, 2, -5, -11, 0, 5, -10, 12, -12, 0, -5,$

where $x^2 - 3x + 1 = 0$. Since the norm of $a_p(g) - a_p(f)$ is divisible by 5 for $p \nmid 675$, this suggests that g is congruent to f modulo 5. Since $a_p(g) = 0$ when $\left(\frac{-15}{p}\right) = -1$ for $p \nmid N$, this suggests that g is induced from a grossencharacter on $\mathbb{Q}(\sqrt{-15})$.

608B:

$E : y^2 = x^3 - 56x + 4848$

$N = 608 = 2^5 19$

$j = -4741632/2476099 = 2^9 3^3 7^3/19^5$

$= \frac{(s^2-5)^3(s^2+5s+10)^3(s+5)^3}{(s^2+5s+5)^5}$ for $s = 2$, so $\overline{\rho}_5$ has image lying in the normalizer of a split Cartan subgroup. It does not have a 5-isogeny as j is not of the form $j = (x^2 + 250x + 3125)^3/x^5$ for $x \in \mathbb{Q}$. Thus, $\overline{\rho}_5$ is split dihedral.

$\Delta = -2^{12} 19^5$

By Ribet's theorem, $\overline{\rho}_5$ is modular of level 32, but there is only one newform $32A$ of level 32 corresponding to an isogeny class of elliptic curves with complex multiplication by -4.

$a_p(g) = [-, 0, -2, 0, 0, 6, 2, 0, 0, -10, 0, -2, 10, 0, 0,$

$a_p(f) = [-, 0, 3, 5, 5, -4, -3, +, 0, 0, -10, 8, 0, 5, -5,$

Conclusions: If $\ell \in D^{-}_{E/\mathbb{Q}}$, $\ell > 3$ and $\ell \nmid N$, we can find at least two distinct normalized eigenforms which are congruent modulo ℓ to f, one which is a quadratic twist of f, and another which is induced from a grossencharacter on an imaginary quadratic field. Question: how often can this occur? This relates to a question of Serre which asks if the union of $S_{E/\mathbb{Q}}$ across all elliptic curves $E/\mathbb{Q}$ without complex multiplication is finite.