Existence of Taylor-Wiles Primes

Michael Lipnowski

Introduction

Let F be a totally real number field, $\overline{\rho} = \overline{\rho_f} : G_F \to GL_2(k)$ be an odd residually modular representation (odd meaning that complex conjugation acts as $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ for every archimedean place).
Let St be the set of places where ρ_f is Steinberg, S_p is the set of places over p, S_∞ the set of archimedean places of F, , and assume it is unramified everywhere else. For the purposes of this write up, all that matters is that $St \cup S_p$ is a finite set of finite places.
Our is to construct certain auxillary sets of places Q of F which have associated deformation rings R_Q. Q will consist of so called *Taylor-Wiles Places.*

Definition. *A place v of F is a **Taylor-Wiles place** if it satisfies the following conditions.*

- $v \notin S \cup S_p$.
- $Nv \equiv 1 \ (p)$.
- *The eigenvalues of $\overline{\rho}(Frob_v)$ are distinct and belong to k.*

Let $R^{\square,\chi}_{Q \cup St \cup S_p}$ be the universal framed deformation ring unramified outside of $Q \cup St \cup S_p$ with fixed determinant $\chi = \chi_p$, the p-adic cyclotomic character.
Let $L^\square$ be the completed tensor product of the universal framed local deformation rings at $v \in St \cup S_p$ of fixed determinant ψ_v and $B^\square$ the completed universal product of their Steinberg quotients (for $v \in St$,) and their ordinary-crystalline quotients for $v \in S_p$.
Let $R^\square_Q = R^{\square,\chi}_{Q \cup St \cup S_p} \otimes_{L^\square} B^\square$. This represents the universal framed deformation $\rho : G_F \to GL_2(R_Q)$ of $\overline{\rho}$ unramified outisde of $Q \cup St \cup S_p$ which is Steinberg at St and ordinary-crystalline at S_p.

Although we do allow ramification at Q, the Taylor-Wiles conditions control it tightly.
Let v be a Taylor-Wiles place and consider $\rho|_{G_{F_v}}$.
$\overline{\rho}$ is unramified at v. So, $\rho(I_v)$ lands inside the 1-units of $GL_2(R_Q)$, which is a pro-p group. But the wild inertia group $W_v \subset I_v$ is a pro-v group and so it gets killed. Thus, the reduction is tamely ramified at v. Even better,

Lemma. $\rho|_{G_{F_v}}$ *is a sum of two (tamely ramified) characters $\eta_1 \oplus \eta_2$.*

Proof. The tame galois group is generated by $\sigma = Frob_v$ and the group I_v. For every $\tau \in I_v$, we have the relation

$$\sigma\tau\sigma^{-1} = \tau^{Nv}. \quad (*)$$

By the Taylor-Wiles assumption on Frobenii, $\overline{\rho}(\sigma)$ has distinct eigenvalues. By Hensel's lemma, we may lift $\overline{\rho}(\sigma)$ so that $\rho(\sigma)$ is diagonal, say $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$,
with respect to some (possibly different) basis. With respect to this basis, express

$$\rho(\tau) = 1 + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

For some $a, b, c, d \in m_Q$. Apply ρ to $(*)$ and expand to get

$$1 + \begin{pmatrix} a & b\alpha\beta^{-1} \\ c\beta\alpha^{-1} & d \end{pmatrix} = \sum_{k=0}^{Nv} \binom{Nv}{k} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^k.$$

Note that for $k \geq 2$, the top right and bottom left entries of the right side summands lie in $m_Q(b, c)$. Thus comparing with these entries on the left side,

$$b(\alpha\beta^{-1} - Nv), c(\beta\alpha^{-1} - Nv) \in m_Q(b, c).$$

But α and β are residually distinct, by assumption. Then by the congruence property of TW places

$$\alpha\beta^{-1} - Nv, \beta\alpha^{-1} - Nv \neq 0 \ (p)$$

implying that both terms are units in R_Q. Thus, $(b, c) \subset m_Q(b, c)$. By Nakayama's Lemma, this implies that $b = c = 0$. Since τ was aribitrary, the claim follows. □

$\mathcal{O}[\Delta_Q]$ Structure on $R_Q^\square$

We have just shown that $\rho|_{G_{F_v}}$ is a sum of two (tamely ramified) characters $\eta_1 \oplus \eta_2$. Choose one, say η.
We know that $\eta|_{I_v}$ has pro-p image. Also by class field theory, it determines a character $\eta' : O_v^\times \to R_Q^{\square\times}$. As the 1-units are pro-v, this is really a map $\eta' : (O_v/v)^\times \to R_Q^{\square\times}$ which factors through the maximal p-power quotient of $(O_v/v)^\times$. Call this maximal p-power quotient Δ_v. Let $\Delta_Q = \prod_{v \in Q} \Delta_v$. Our choice of η defines an action of Δ_Q on R_Q, thus giving R_Q the structure of an $\mathcal{O}[\Delta_Q]$-module.

We still haven't constructed the set of primes Q. Actually, we want to construct a family of such $Q = Q_n$ of the following sort:
For fixed positive integers g, h satisfying $\dim B^\square = 1 + h + l - g$ (remember that $B^\square$ is the framed ring of Steinberg and ord-cryst conditions),

- $|Q_n| = h$
- $Nv = 1 \ (p^n)$
- $R_{Q_n}^\square$ is topological generated by g elements over $B^\square$.

Note that the congruence condition $Nv = 1$ (p^n) means that Δ_v is $p-$power cyclic of order divisible by p^n. Thus, after a choice of generators for these cyclic groups, the $\mathcal{O}[\Delta_Q]$-module structure on $R_Q^\square$ is equivalently an $\mathcal{O}[[T_1, ..., T_h]]/((T_1+1)^{p^{a_1}} - 1, ..., (T_h+1)^{p^{a_h}} - 1)$-module structure, where all $a_i \geq n$.
There are no obvious maps between the R_{Q_n}. But by the magic of the patching, we will find a subset of the R_{Q_n} which form a kind of inverse system with limit $R_\infty^\square$. We dream that by "letting $n \to \infty$", we'll give $R_\infty^\square$ the structure of a free $\mathcal{O}[[T_1, ..., T_h]]$-module.
A couple remarks about these conditions:

1) The explicit values

$$\begin{aligned} h &= \dim H^1(G_{F,St\cup S_p}, ad^0\overline{\rho}(1)) \\ g &= h - [F:\mathbb{Q}] + |St| + |S_p| - 1 \end{aligned}$$

will suffice.

2) Our stipulation that $\dim B^\square = 1 + h + l - g$ will only appear natural once we dive into the patching argument.

3) The g we will construct is actually the relative topological dimension of $R_{Q_n}^\square$ over $L^\square$, which will certainly suffice.

Construction of the TW Sets

From now on, we will assume that

$$\overline{\rho}|_{G_{F(\zeta_p)}} \text{is absolutely irreducible.}$$

This cheaply implies the following apparently much stronger fact.

Lemma. *$\overline{\rho}|_{G_{F(\zeta_{p^n})}}$ is absolutely irreducible.*

Proof. Our standing assumption is that $\overline{\rho}|_{G_{F(\zeta_p)}}$ is absolutely irreducible.
Note that $H = G_{F(\zeta_{p^n})}$ is a normal subgroup of $G = G_{F(\zeta_p)}$. Thus, the restriction $\overline{\rho}|_H$ is semisimple. Indeed, if W is an invariant subspace, then

$$\bigoplus_{G/H - 1.H} gW$$

is an invariant complement.
Suppose $\overline{\rho}|_H$ is not irreducible. Then it is the direct sum of two characters. Since V, as a G-module, is absolutely irreducible, G/H must permute these characters transitively. But G/H is a p-group, and so it cannot act transitively on a 2 element set (for any $p > 2$, which we have assumed). Thus, the two characters are the same.
This implies that every line in V is stabilized by H. But there are $|\mathbb{P}(V)(k)| = |k| + 1$ of them. So the number of them is prime to p. Hence, some orbit of G/H on the set of k-lines in V has size prime to p. But the size of the orbit must also divide $|G/H|$, which is p-power. Hence, this orbit has size 1, i.e. there is an H-stable line which is G/H-stable. This line is then G-stable, contradicting the irreducibility of V.
The same argument carries out mutatis mutandis after first making a finite extension of the ground field k of V. Thus, $\overline{\rho}|_H$ is indeed absolutely irreducible. $\square$

We'll now prove our main lemma of interest.

Theorem (DDT, Lemma 2.49). *Let $h = \dim H^1(G_{F,St\cup S_p}, ad^0(\overline{\rho}(1)))$. For every n, we can construct a set Q_n of Taylor-Wiles places, i.e.*

(1) For each $v \in Q_n, Nv = 1\ (p^n)$.

(2) For each $v \in Q_n, \overline{\rho}(Frob_v)$ has distinct k-rational eigenvalues.

(3) $|Q_n| = h$.

Proof. An easy calculation shows that if $\overline{\rho}(Frob_v)$ is a Taylor-Wiles place, then $\dim H^1(k_v, ad^0(\overline{\rho})(1)) = 1$.
Indeed, for any σ in $G_{F,St\cup S_p}$, if σ has (generalized) eigenvalues α, β then $ad^0(\overline{\rho})(\sigma)$ has (generalized) eigenvalues $1, \alpha\beta^{-1}, \beta\alpha^{-1}$. Thus, if $\overline{\rho}(Frob_v)$ has distinct eigenvalues, the space $ad^0(V)/(Frob_v - 1)ad^0(V)$ is one dimensional. Since a v-unramified cocycle is uniquely determined by its value on $Frob_v$, we get that $\dim H^1(k_v, ad^0(\overline{\rho})(1)) = 1$.
Thus, it suffices to show that the restriction map

$$H^1(G_{F,St\cup S_p}, ad^0(\overline{\rho})(1)) \to \oplus_{v\in Q_n} H^1(k_v, ad^0(\overline{\rho})(1))$$

is an isomorphism. Then equating dimensions shows that condition (3) is fulfilled.
To do this, it suffices to show that for any global cocycle ψ there exists a $v = v_\psi$ satisfying (1) and (2) such that $res_v(\psi) \neq 0$. For then we could apply this to the elements of a basis (of size h) for the left side, and the corresponding set of places $\{v_\psi\}$ would consistute a TW set.
Instead we'll show that we can find $\sigma \in G_{F,St\cup S_p}$ satisfying the following:

(1') $\sigma|_{G_{F(\zeta_p)}} = 1$.

(2') $ad^0\overline{\rho}(\sigma)$ has an eigenvalue other than 1.

(3') $\psi(\sigma) \notin (\sigma - 1)ad^0\overline{\rho}(1)$.

Indeed, all three of the above conditions are open conditions in $G_{F,St\cup S_p}$. But by the Chebotarev density theorem, we any non-empty open set contains some $Frob_v$. This v will do.

Let F_0 be the fixed field of the kernel of $ad^0\overline{\rho}$ and let $F_m = F_0(\zeta_{p^m})$.

Claim. *$\psi(G_{F_n})$ is non-zero.*

Later, we'll even show that its k-span is a non-zero $Gal(F_n/F(\zeta_{p^n}))$-submodule of $ad^0\overline{\rho}$. From this, we can leverage information from the irreducibility of $\overline{\rho}|_{G_{F(\zeta_{p^n})}}$ just proven.

Proof. In this claim and what follows, assume $n > 0$ so that the cyclotomic character is trivial when restricted to G_{F_n}. There is an inflation-restriction sequence

$$0 \to H^1(G_{F_n/F}, ad^0\overline{\rho}(1)) \xrightarrow{inf} H^1(G_F, ad^0\overline{\rho}(1)) \xrightarrow{res} H^1(G_{F_n}, ad^0\overline{\rho}(1)).$$

Thus, it suffices to prove that the leftmost term is zero. For then, $\psi|_{G_{F_n}}$ is a non-zero cohomology class, and so is certainly not identically 0.
We can sandwich the left most term in another inflation-restriction sequence:

$$0 \to H^1(G_{F_0/F}, (ad^0\overline{\rho}(1))^{G_{F_0}}) \xrightarrow{inf} H^1(G_{F_n/F}, ad^0\overline{\rho}(1)) \xrightarrow{res} H^1(G_{F_n/F_0}, ad^0\overline{\rho}(1))^{G_{F_0/F}}. \ (*)$$

where the action of $g \in G_{F_0/F}$ on the third term is given by $\eta \mapsto (h \mapsto g^{-1}\eta(ghg^{-1}))$.

- Third term of (*)
  There is a restriction-corestriction sequence

$$H^1(G_{F_n/F_0}, ad^0\overline{\rho}(1)) \xrightarrow{res} H^1(G_{F_n/F_1}, ad^0\overline{\rho}(1)) \xrightarrow{cores} H^1(G_{F_n/F_0}, ad^0\overline{\rho}(1))$$

  and the composition is multiplication by $|G_{F_1/F_0}|$. This number is $\leq p-1$ and so is prime to p. Hence, res is injective. It also sends $G_{F_0/F}$-invariants to $G_{F_0/F}$-invariants. Thus, it suffices to show that $H^1(G_{F_n/F_1}, ad^0\overline{\rho}(1))^{G_{F_0/F}}$ is zero.

  - G_{F_n/F_1} is naturally a subgroup of the commutative quotient $G_{F(\zeta_{p^n})/F}$ of G_F (given just by restricting automorphisms to $F(\zeta_{p^n})$). The conjugation action is compatible with this restriction. Thus the conjugation action on G_{F_n/F_1} is trivial since the latter quotient of G_F is abelian.
    Note that G_{F_n/F_1} acts trivially on $ad^0\overline{\rho}(1)$. Hence,

$$H^1(G_{F_n/F_1}, ad^0\overline{\rho}(1))^{G_{F_0/F}} = Hom(G_{F_n/F_1}, ad^0\overline{\rho}(1))^{G_{F_0/F}} = Hom(G_{F_n/F_1}, ad^0\overline{\rho}(1)^{G_{F_0/F}}).$$

    But $ad^0\overline{\rho}(1)^{G_{F_0/F}} = 0$.
    Indeed, any $G_{F(\zeta_{p^n})}$-invariant element of $ad^0\overline{\rho}(1)$ is equivalently a trace 0 intertwining operator $V \to V(1)$ (V the underlying vector space of ad^0). But $n > 0$, so the action of the cyclotomic character is trivial. So this is actually an intertwining operator $V \to V$. But V is an irreducible $G_{F(\zeta_{p^n})}$-module, and so any self-intertwining operator is scalar and so must be 0 by our trace 0 assumption ($p > 3$ by our standing assumptions).

  Hence, the third term of $(*)$ is 0.

- First term of (*)

  - $(ad^0\overline{\rho}(1))^{G_{F_0/F}}$ is trivial unless $F_0 \supset F(\zeta_p)$. This is because for any place v with $Nv \neq 1\ (p), ad^0\overline{\rho}(Frob_v)$ fixes something but $\chi_p(Frob_v) \neq 1$. So, we assume that

$$G_{F_0/F} \to G_{F(\zeta_p)/F} \to 0.$$

    In particular, $G_{F_0/F}$ has a non-trivial quotient and so is not a non-abelian simple group.
  - Since $(ad^0\overline{\rho}(1))^{G_{F_0/F}}$ has p-power order, we also have an injection

$$0 \to H^1(G_{F_0/F}, (ad^0\overline{\rho}(1))^{G_{F_0}}) \xrightarrow{res} H^1(P, (ad^0\overline{\rho}(1))^{G_{F_0}}),$$

    where P is the Sylow p-subgroup of $G_{F_0/F}$. Thus, we can assume that P is non-trivial, i.e. that p divides $|G_{F_0/F}|$.
  - Finally, since F_0 is the field cut out by $ad^0\overline{\rho}, G_{F_0/F}$ is isomorphic to the projective image of $\overline{\rho}$.

We can put these facts to good use in conjunction with an explicit characterization of finite subgroups of $PGL_2(\overline{\mathbb{F}}_p)$.

List of Finite Subgroups H of $PGL_2(\overline{\mathbb{F}}_p)$ [**EG, II.8.27**]

– H is conjugate to a subgroup of the upper triangular matrices.

– H is conjugate to $PGL_2(\mathbb{F}_{p^r})$ or $PSL_2(\mathbb{F}_{p^r})$ for some $r \geq 1$.

– H is isomorphic to A_4, A_5, S_4, or $D_{2r}, p \nmid r$ for $r \geq 2$. Furthermore, if H is isomorphic to $D_{2r} = \langle s, t | s^2 = t^r = 1, sts = t^{-1} \rangle$, then it is conjugate to the image of

$$s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} t \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix},$$

where ζ is a primitive r^{th} root of unity.

We can eliminate all of these possibilities, one by one.

– The projective image H cannot be conjugate to a subgroup of the upper triangular matrices, for then $\overline{\rho}|_{G_{F(\zeta_p)}}$ would not be absolutely irreducible.

– Our assumptions $p > 5$ and p divides $|G_{F_0/F}|$ preclude the possibilities $H \cong A_4, A_5, S_4, D_{2r}, p \nmid r$.

– $PSL_2(\mathbb{F}_{p^r})$ is simple for $p > 5$. Thus, it cannot have a quotient, namely $G_{F(\zeta_p)/F}$, which is non-trivial.

– Suppose $H = im(\overline{\rho}) \cong PGL_2(\mathbb{F}_{p^r})$. The only non-trivial quotient of $PGL_2(\mathbb{F}_{p^r})$ is order 2. But $G_{F_0/F}$ cannot have a quotient of order 2.
If it did, there would be an exact sequence

$$1 \to Z \to im(\overline{\rho}) \to im(ad^0(\overline{\rho})) \to 1,$$

with Z a central subgroup of $GL_2(k)$ and $im(ad^0(\overline{\rho}))$ either order 1 or 2. But then any pre-image A of the non-trivial element of $im(ad^0(\overline{\rho}))$ and Z generate $im(\overline{\rho})$. But A has an invariant subspace (possibly after a quadratic extension). So that means $im(\overline{\rho})$ does too, contradicting the absolute irreducibility of $\overline{\rho}$.

Since none of these are possible, we must have the first term of $(*)$ being 0 after all.

We conclude that the second term of $(*)$ is 0 as well, which is what we wanted; this proves that $\psi(G_{F_n})$ is indeed non-zero. □

We can say more. For $\tau, \tau' \in G_{F_n}, \sigma \in G_{F(\zeta_{p^n})}$, repeated use of the cocycle relation gives

$$\begin{aligned} \psi(\sigma\tau\sigma^{-1}) &= \psi(\sigma) + \psi(\tau\sigma^{-1}) \\ &= \psi(\sigma) + \sigma\psi(\tau) + \sigma\tau\psi(\sigma^{-1}) \\ &= \psi(\sigma) + \sigma\psi(\tau) + \sigma\psi(\sigma^{-1}) = \sigma\psi(\tau). \end{aligned}$$

Note: the second last equality holds because τ acts trivially on $ad^0\overline{\rho}(G_{F_n})$. Also,

$$\psi(\tau) + \psi(\tau') = \tau'\psi(\tau) + \psi(\tau') = \psi(\tau\tau').$$

Thus, the k-span of $\psi(G_{F_n})$ is in fact a non-zero $G_{F_n/F(\zeta_{p^n})}$-submodule of $ad^0\overline{\rho}$.

Next, we'll find an element $g \in G_{F_n/F(\zeta_{p^n})}$ such that $\overline{\rho}(g)$ has distinct eigenvalues and which fixes an element of $k.\psi(G_{F_n})$. We do this by the explicit classification of possible projective images, i.e. we'll show that for any subgroup H which could possibly be the projective image of $\overline{\rho}$, there is an element of H with distinct eigenvalues which fixes an element of $k.\psi(G_{F_n})$.

- Note first that if we can prove the result for some subgroup $H \subset H'$, then it true for putative projective image H' as well. Also, the "exceptional" cases A_4, S_4, and A_5 all contain D_4 and the projective image cannot be contained in an upper triangular subgroup (due to the absolute irreducibility of $\overline{\rho}|_{G_{F(\zeta_{p^n})}}$. Thus, in view of the preceding classification of finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$, it suffices to check the following cases:

- $\underline{PSL_2(\mathbb{F}_{p^r})}$
  ad^0 is simple under the action of $PSL_2(\mathbb{F}_{p^r})$. Thus, $k.\psi(G_{F_n}) = ad^0$ and $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ fixes $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in ad^0 = k.\psi(G_{F_n})$. Since $p > 5$, we can certainly find $\alpha \neq \alpha^{-1}$.

- $\underline{D_4}$
  ad^0 decomposes as $V_1 \oplus V_2 \oplus V_3$, where

$$V_1 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, V_2 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle, V_3 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

  D_4 acts as ± 1 on each V_i. Furthermore, by our explicit description of the image of dihedral groups, each non-trivial element has distinct eigenvalues (of ± 1). Since the only possible invariant subspaces of ad^0 are then $\oplus_{i \in I} V_i$ for some $I \subset \{1, 2, 3\}$, it follows that some element $h \in D_4$ with distinct eigenvalues fixes an element of $k.\psi(G_{F_n})$.

- $\underline{D_{2r}, r \text{ odd}}$
  ad^0 decomposes as $W_1 \oplus W_2$ where

$$W_1 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, W_2 = \left\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

  W_1 is fixed by $\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ fixes $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

  Since $ad^0 = W_i$ or $W_1 \oplus W_2$, it follows again that some $h \in D_{2r}$ with distinct eigenvalues fixes an element of $k.\psi(G_{F_n})$.

Having found such a g, it must certainly fix a non-zero element of $\psi(G_{F_n})$ itself, say $\psi(\tau_0)$.

- Indeed, as an $\mathbb{F}_p$-vector space, the $k.\psi(G_{F_n})$ is isomorphic to $k \otimes_{\mathbb{F}_p} \psi(G_{F_n})$. But then if $k_1, ..., k_m$ forms a basis for k over $\mathbb{F}_p$, we can express the fixed element m of $k.\psi(G_{F_n})$ as $m = k_1\psi(\tau_1) + ... + k_n\psi(\tau_n)$, where at least one $\psi(\tau_i) \neq 0$. If m is fixed by g, then

$$k_1((g-1)\psi(\tau_1)) + ... + k_n((g-1)\psi(\tau_n)) = 0.$$

  But linear independence implies that $(g-1)\psi(\tau_i) = 0$, which is what we wanted.

Choose a lift σ_0 of g to the absolute Galois group.
For $\tau \in G_{F_n}$, we have

$$\psi(\tau\sigma_0) = \tau\psi(\sigma_0) + \psi(\tau) = \psi(\sigma_0) + \psi(\tau).$$

- If $\psi(\sigma_0) \notin (\sigma_0 - 1)(ad^0\overline{\rho}(1))$, then take $\tau = 1$.
- Otherwise, choose $\tau = \tau_0$. For this choice, $\psi(\tau_0) \notin (\sigma_0 - 1)ad^0\overline{\rho}(1)$. For suppose $(\sigma_0 - 1)x = \psi(\tau_0) \neq 0$. Applying $\sigma_0 - 1$ to both sides, our construction of τ_0 gives

  $$(\sigma_0 - 1)^2 x = (\sigma_0 - 1)\psi(\tau_0) = 0.$$

  But σ_0 acting on ad^0 is semisimple and has eigenvalue 1 with multiplicity 1 (since $\overline{\rho}(\sigma_0)$ has distinct eigenvalues) . Thus, $(\sigma_0 - 1)x = 0$, implying that $\psi(\tau_0) = 0$, contrary to our construction.

Thus, in both cases

$$\psi(\tau\sigma_0) \notin (\sigma_0 - 1)ad^0\overline{\rho}(1) = (\tau\sigma_0 - 1)ad^0\overline{\rho}(1).$$

So we've finally constructed the element $\sigma = \tau\sigma_0$ that we sought in the first place. □

Number of Topological Generators for $R^{\square,\chi}_{Q_n \cup St \cup S_p}$ over $L^{\square}$

We now have all of the pieces in place to compute the relative tangent space dimension of $R^{\square,\chi}_{Q_n \cup St \cup S_p}$ over $L^{\square}$, both defined as in the introduction.

Lemma (FFGS, 3.2.2). *Let $h^1(G_{F,St\cup S_p\cup S_\infty}, ad^0(V))$ denote the k-dimension of*

$$\ker(H^1(G_{F,St\cup S_p\cup S_\infty}, ad^0(V)) \to \prod_{v\in St\cup S_p} H^1(G_{F_v}, ad^0(V))).$$

For $v \in St \cup S_p$, let $\delta_v = \dim_k H^0(G_{F,St\cup S_p\cup S_\infty}, adV)$ and $\delta_F = \dim_k H^0(G_{F,St\cup S_p\cup S_\infty}, adV)$. Then $R^{\square,\chi}_{F,St\cup S_p\cup S_\infty}$ is the quotient of a power series ring over $L^{\square}$ in

$$g = h^1(G_{F,St\cup S_p\cup S_\infty}, ad^0(V)) + \sum_{v\in St\cup S_p} \delta_v - \delta_F.$$

variables.

Proof. Let our vector space V have fixed basis β.
An element of the relative tangent space corresponds to a deformation of V to a finite free $k[\epsilon]$-module $\tilde{V}$ together with a choice of bases $\tilde{\beta}_v$ lifting β such that for each $v \in St \cup S_p$, the pair $(\tilde{V}|_{G_{F_v}}, \beta_v)$ is isomorphic to $(V \otimes_k k[\epsilon], \beta \otimes_k 1)$.
For fixed choices of bases, the space of such deformations is given by

$$ker(H^1(G_{F,St\cup S_p\cup S_\infty}, ad^0(V)) \to \prod_{v\in St\cup S_p} H^1(G_{F_v}, ad^0(V))).$$

Given such a deformation, $\tilde{V}$, the space of possible choices for a bases is the space of G_{F_v} automorphisms of $(V \otimes_k k[\epsilon], \beta \otimes_k 1)$; such an automorphism reduces to 1 mod (ϵ) and so is of the form $1 + \epsilon M$ for some G_{F_v}-equivariant $M \in ad(V)$, i.e. $M \in H^0(G_{F_v}, adV)$.
The same reasoning shows that two collections $\{\beta_v\}_{v\in St\cup S_p}$ and $\{\beta'_v\}_{v\in St\cup S_p}$ determine the same framed deformation if they differ by an element of $H^0(G_{F,St\cup S_p\cup S_\infty}, adV)$. The lemma follows.
□

Now we compute this h^1, the dimension of a Selmer group, via the Wiles Product formula.

Lemma (FFGS, 3.2.5). *Set* $g = \dim_k H^1(G_{F,S_p \cup St}, ad^0\overline{\rho}(1)), ad^0\overline{\rho}(1)) - [F:\mathbb{Q}] + |St| + |S_p| - 1$. *For each positive integer n, there is a finite set of primes* Q_n *of* F *which is disjoint from* $St \cup S_p$ *and such that*

(1) If $v \in Q_n$*, then* $Nv = 1$ (p^n) *and* $\overline{\rho}(Frob_v)$ *has distinct eigenvalues.*

(2) $|Q_n| = \dim_k H^1(G_{F,S_p \cup St}, ad^0\overline{\rho}(1))$. *Also,* $R^{\square}_{Q_n}$ *is topolgoically generated by g elements as a* $B^{\square}$*-algebra.*

Proof. We define a set of local conditions to compute this relative dimension, the dimension of a Selmer group. Namely, let

$$H^1_{\mathcal{L}_v} = \begin{cases} 0 & \text{if } v \in St \cup S_p \\ H^1(G_{F_v}, ad^0\overline{\rho}) & \text{otherwise.} \end{cases}$$

Write $H^1_{\mathcal{L}_{Q_n}}$ (resp. $H^1_{\mathcal{L}^{\perp}_{Q_n}}$) for the set of classes which restrict to $H^1_{\mathcal{L}_v}$ (resp. $H^1_{\mathcal{L}^{\perp}_v}$) for each $v \in St \cup S_p \cup Q_n$. ("$\perp$" denoting the annihilator under Tate local duality).
The main result from the previous section shows that we can find a set of primes Q_n satisfying condition (1) and the first part of condition (2). Furthermore, any class in $H^1_{\mathcal{L}^{\perp}_{Q_n}}$ restricts to 0 in $H^1(G_{F_v}, ad^0\overline{\rho}(1))$. By our choice of primes, this implies that $H^1_{\mathcal{L}^{\perp}_{Q_n}} = 0$.

By the Wiles Product Formula, we get

$$|H^1_{\mathcal{L}_{Q_n}}| = \frac{H^0(G_{F,St\cup S_p \cup S_\infty}, ad^0\overline{\rho})}{H^0(G_{F,St\cup S_p \cup S_\infty}, ad^0\overline{\rho}(1))} \prod_{v \in St \cup S_p \cup S_\infty} \frac{H^1_{\mathcal{L}_v}}{H^0(G_{F_v}, ad^0\overline{\rho})}.$$

- Global terms
  An element of $H^0(G_{F,St\cup S_p \cup S_\infty}, ad^0\overline{\rho})$ corresponds to a trace 0 self-intertwining operator of V. Since $\overline{\rho}|_{G_{F(\zeta_p)}}$ is absolutely irreducible, any self-intertwining operators are scalars. But the only trace 0 scalar matrix is 0 (for $p > 2$).
  Similarly, an element of $H^0(G_{F,St\cup S_p \cup S_\infty}, ad^0\overline{\rho}(1))$ corresponds to an intertwining operator $V \to V(1)$ between irreducible $G_{F(\zeta_p)}$-modules. Either they are not isomorphic, in which case only the 0 operator can intertwine them, or they are isomorphic, in which case the above paragraph applies.

- $v \in St \cup S_p$
  $ad^0(V)$ is a summand of $ad(V)$ for $p > 2$. So, the terms in the product corresponding to $v \in St \cup S_p$ in the product formula contribute $|k|^{1-\delta_v}$.

- $v \in S_\infty$

- $v \in Q_n$

$$\frac{H^1(G_{F_v}, ad^0\overline{\rho})}{H^0(G_{F_v}, ad^0\overline{\rho})} = H^2((G_{F_v}, ad^0\overline{\rho})) \times \text{local Euler characteristic}^{-1}.$$

  The H^2 term equals $H^0(G_{F_v}, ad^0\overline{\rho}(1))$ by Tate local duality. The local Euler characteristic, which equals $[O_v : |ad^0(V)|O_v]^{-1}$ by the local Euler characteristic formula, is 1 since $|ad^0(V)|$ is prime to $v \in Q_n$. Hence, the product formula terms for $v \in Q_n$ equal $H^0(G_{F_v}, ad^0\overline{\rho}(1))$.

Since $\overline{\rho}(Frob_v)$ had distinct eigenvalues, there is a 1-dimensional subspace of $ad^0(V)$ fixed by $ad^0\overline{\rho}(Frob_v)$. Since $\overline{\rho}|_{G_{F_v}}$ is unramified, $H^0(G_{F_v}, ad^0\overline{\rho}(1))$ is 1-dimensional.

- $\underline{S_\infty}$

  By one of our standing assumptions, $\overline{\rho}$ is odd, i.e. for archimedean places $v, \overline{\rho(c)}$ can represented as a matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ with respect to some basis. Hence, $ad^0\overline{\rho}(c)$ is can be diagonalized to $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. But G_{F_v} is cyclic of order 2, generated by c. Hence, the space of cocycles is just $\ker(ad^0\overline{\rho}(c)+1)$, which is 2-dimensional, and the space of coboundaries is $im(ad^0\overline{\rho}(c)-1)$, which is 2-dimensional. Hence $H^1(G_{F_v}, ad^0\overline{\rho}) = 0$. Also, $H^0(G_{F_v}, ad^0\overline{\rho})$ is the 1-eigenspace of $ad^0\overline{\rho}(c)$, and so is 1-dimensional.

Adding everything together, we get

$$\begin{aligned}
h^1(G_{F,St\cup S_p\cup S_\infty}, ad^0(V)) &= \dim_k H^1_{\mathcal{L}_{Q_n}} \\
&= 0 + \sum_{v\in St\cup S_p}(1-\delta_v) + \sum_{v\in Q_n} 1 + \sum_{v\in S_\infty} -1 \\
&= |St| + |S_p| - \sum_{v\in St\cup S_p} \delta_v + |Q_n| + [F:\mathbb{Q}] \\
&= |St| + |S_p| - \sum_{v\in St\cup S_p} \delta_v + \dim_k H^1(G_{F,St\cup S_p}, ad^0\overline{\rho}(1)) + [F:\mathbb{Q}]
\end{aligned}$$

Combining with the previous lemma gives that

$$g = \dim_k H^1(G_{F,St\cup S_p}, ad^0\overline{\rho}(1)) + |St| + |S_p| + [F:\mathbb{Q}] - 1,$$

as desired. □

We can conclude that $R_Q^\square$ is generated by g elements as a $B^\square$ algebra as well. Thus, we are finally done our construction of TW primes.

References

DDT H. Darmon, F. Diamon, R. Taylor. *Fermat's Last Theorem.* Current Developments in Mathematics 1 (1995), International Press, pp. 1-157.

FFGS M. Kisin. *Moduli of Finite Flat Group Schemes and Modularity.* Annals of Math. 170(3) (2009), 1085-1180.

EG B. Huppert. *Endliche Gruppen I.* Grundlehren Math. Wiss. 134 (1983), Springer-Verlag, New York, Berlin, Heidelberg.

S. Shah. *Framed Deformation and Modularity.* Harvard Undergraduate Thesis (2009). Available at http://math.harvard.edu/theses/senior/shah/shah.pdf