A PROOF OF FERMAT'S LAST THEOREM

1. Fontaine's argument

See [F] and [Sc].

Theorem 1.1. *Suppose that* $\overline{r}: G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_3)$ *is a continuous representation unramified outside* 2 *and* 3 *such that*

- $\#\overline{r}(I_{\mathbb{Q}_2})|2$;
- $\overline{r}|_{G_{\mathbb{Q}_3}}$ *is Fontaine-Laffaille with Hodge-Tate numbers* $\{0, 1\}$.

Then there is an exact sequence

$$(0) \longrightarrow \overline{\mathbb{F}}_3 \longrightarrow \overline{r} \longrightarrow \overline{\mathbb{F}}_3(\overline{\epsilon}_3^{-1}) \longrightarrow (0).$$

Proof: Sketch: Let $L = \overline{\mathbb{Q}}^{\ker \overline{r}}[\zeta_3, \sqrt[3]{2}]$. As in [F] one checks that

$$|D_{L/\mathbb{Q}}|^{1/[L:\mathbb{Q}]} < 2\sqrt{27}$$

and so from the Odlyzko bound we have $[L : \mathbb{Q}[\zeta_3, \sqrt[3]{2}]] < 4$. Using class field theory, one can check that $\mathbb{Q}[\zeta_3, \sqrt[3]{2}]$ has no quadratic extension unramified outside 3, and so $[L : \mathbb{Q}[\zeta_3]]$ is a power of 3. One deduces that $\overline{r}$ is reducible, and the JH factors must be 1 and $\overline{\epsilon}_3^{-1}$. One then uses Kummer theory to see that there is no nonsplit extension of $\overline{\epsilon}_3^{-1}$ by 1 which is FL at 3 and unramified away from 6. □

Corollary 1.2. *Suppose that* $r : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_3)$ *is a continuous semi-simple representation unramified away from* 2 *and* 3 *such that*

- $r|_{I_{\mathbb{Q}_2}}^{\mathrm{ss}} \sim 1 \oplus \epsilon_3^{-1}$
- $r|_{G_{\mathbb{Q}_3}}$ *is crystalline with Hodge-Tate numbers* $\{0, 1\}$.

Then $r \sim 1 \oplus \epsilon_3^{-1}$.

Proof: If r were irreducible we could choose a lattice such that the reduction $\overline{r}$ of r with respect to this lattice is either irreducible or a non-split extension of 1 by $\overline{\epsilon}_3^{-1}$. This would contradict the theorem. The corollary now follows easily. □

2. Automorphic forms and their associated Galois representations

I think it suffices for the most part to work in the following generalilty. Let F denote a totally real number field of even degree and let D denote the quaternion algebra with centre F ramified at exactly the infinite places of F. Let S denote a finite set of finite places of F. We will write $U_0(S)$ for the subgroup of $GL_2(\widehat{\mathcal{O}}_F)$ consisting of matrices which are upper triangular modulo every element of S. We will also write $U_1(S)$ for the subgroup of $U_0(S)$ consisting of matrices whose reduction modulo v has equal diagonal entries for all $v \in S$. We will be interested in the following spaces of

$$S(U_0(S),A) = \{\varphi : (D^\times \backslash (D \otimes \mathbb{A}^\infty)^\times / (\mathbb{A}_F^\infty)^\times U_0(S) \rightarrow A\}$$

and

$$S(U_1(S),A) = \{\varphi : (D^\times \backslash (D \otimes \mathbb{A}^\infty)^\times / (\mathbb{A}_F^\infty)^\times U_1(S) \rightarrow A\}.$$

[We may also need to consider some open compact subgroups intermediate between $U_0(S)$ and $U_1(S)$.]

If $v \notin S$ is a prime of F we set $T_v = [U_1(S) \begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix} U_1(S)]$, where ϖ_v is a uniformizer at v. If $v \in S$ and $\alpha \in \mathcal{O}_{F,v} - \{0\}$ we set $U_{v,\alpha} = [U_1(S) \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} U_1(S)]$. Note that these operators all commute and that $U_{v,\alpha} U_{v,\beta} = U_{v,\alpha\beta}$.

Theorem 2.1. *Suppose that F is a totally real number field of even degree, that l is a prime and that S is a finite set of primes of F not dividing l. Suppose also that $0 \neq f \in S(U_1(S), \overline{\mathbb{Q}}_l)$ is an eigenvector for the Hecke operators T_v for $v \notin S$ and $U_{v,\alpha}$ for $v \in S$ and $\alpha \in \mathcal{O}_{F,v} - \{0\}$; with eigenvalues t_v and $u_{v,\alpha}$ respectively. Suppose moreover that l is unramified in F. [This condition is presumably unnecessary, but fine for our purposes.] Then there is a continuous representation*

$$r_f : G_F \longrightarrow GL_2(\overline{\mathbb{Q}}_l)$$

with the following properties:

1. $\det r_f = \epsilon_l^{-1}$.
2. *If v is a prime of F not in S and not dividing l, then r_f is unramified at v and $\mathrm{tr}\, r_f(\mathrm{Frob}_v)$ equals the eigenvalue of T_v on f.*
3. *If $v | l$ then $r_f|_{G_{F_v}}$ is crystalline with Hodge-Tate numbers $\{0,1\}$.*
4. *If $v \in S$ then there is an extension*

$$(0) \longrightarrow \chi_v \longrightarrow r_f|_{G_{F_v}} \longrightarrow \epsilon_l^{-1}\chi_v^{-1} \longrightarrow (0),$$

where χ_v is a tame character of G_{F_v} characterized by $\chi_v(\mathrm{Art}\,\alpha) = u_{v,\alpha}$ for all $\alpha \in \mathcal{O}_{F,v} - \{0\}$.

(We are using geometric Frobenius elements.)

How does one go about proving this? First one uses Jacquet-Langlands to switch to a quaternion algebra ramified at all but 2 infinite places. I would guess that the trace formula argument in this case can be made at finite level in a relatively elementary manner. This is the sort of argument used by Eichler a long time ago. On the side of the Shimura surface one could use the topological trace formula, see eg [GM] (although this paper is mostly concerned with boundary terms, which we can ignore - there may be better references). Then looking at the cohomology of the corresponding Shimura surface one produces a 4-diml Galois representation R_f. In fact one has to go from the Shimura surface to to a unitary group Shimura surface to get a PEL type moduli problem, but there is a close relationship between the two. We only need to control the local behaviour of R_f almost everywhere. (If it simplifies things one could assume $[F:\mathbb{Q}] > 2$.)

Then one would use level raising congruences to reduce to the case that for some $v_0 \in S$ we have $u_{v_0,\alpha} = 1$ for $\alpha \in \mathcal{O}_{F,v_0}^\times$ and $u_{v_0,\varpi_{v_0}} = \pm 1$. (See [T].) To find suitable primes at which to raise the level we may need the existence of R_f.

Finally in the special case alluded to here one again uses Jacquet-Langlands to switch to a quaternion algebra ramified at v_0 and all but one infinite place. The cohomology of this Shimura curve, or a closely related unitary group Shimura curve will give the desired r_f. One will need to analyse its bad reduction, but only in the relatively easy case of square free level.

We will call $r : G_F \to GL_2(\overline{\mathbb{Q}}_l)$ *automorphic over F of weight 2 and level $U_1(S)$* if it arises in this way for some f. We will call $\overline{r} : G_F \to GL_2(\overline{\mathbb{F}}_l)$ *automorphic over F of weight 2 and level $U_1(S)$* if it has an l-adic lift which is.

3. Base change

Theorem 3.1. *Suppose that E/F is a finite soluble Galois extension of totally real fields with $[F:\mathbb{Q}]$ even, l is a prime, S is a finite set of places of F not dividing l and that*

$$r : G_F \longrightarrow GL_2(\overline{\mathbb{Q}}_l)$$

is a continuous representation such that

- *r unramified outside S and l;*
- *r is crystalline with Hodge-Tate numbers $\{0,1\}$ at all places above l;*
- *if $v \in S$ then $r|_{G_{F_v}}^{\mathrm{ss}} = \chi_v \oplus \epsilon_l^{-1}\chi_v^{-1}$, where χ_v is, at worst, tamely ramified.*
- *$\det r = \epsilon_l^{-1}$;*
- *$r|_{G_E}$ is absolutely irreducible.*

Then $r|_{G_E}$ is automorphic over E of weight 2 and level $U_1(S_E)$ if and only if r is automorphic over F of weight 2 and level $U_1(S)$ (where S_E denotes the set of primes of E above S).

Theorem 3.2. *Suppose that F is an even degree totally real number field and that E is an totally imaginary quadratic extension of F. Let l be a prime such that all primes of F above l are unramified in E, and let L be a finite extension of $\mathbb{Q}_l$. Suppose that*

$$\theta : G_E \longrightarrow L^\times$$

is a continuous character such that

- *$\theta \circ V_{G_F/G_E} = \epsilon_l^{-1}\delta_{E/F}$, where $V_{G_F/G_E} : G_F^{\mathrm{ab}} \to G_E^{\mathrm{ab}}$ denotes the transfer map and $\delta_{E/F}$ denotes the non-trivial character of $\mathrm{Gal}\,(E/F)$.*
- *θ is crystalline at all primes above l and $\theta \oplus \theta^c$ has Hodge-Tate numbers $\{0,1\}$,*
- *θ is unramified away from l.*

Then $\mathrm{Ind}\,_{G_E}^{G_F}\theta$ is automorphic over F of weight 2 and level $U_0(\emptyset)$.

The first of these results is easily reduced to the case that E/F is cyclic of prime degree p. Then both results should follow from the usual trace formula argument for base change. It is not clear to me whether it would suffice to work at level $U_1(S)$ - maybe one has to go outside this to get the desired trace identities? The 'only if' part of the first theorem probably requires a multiplicity one result, that presumably has to be proved by using some form of Jacquet-Langlands to compare with Hilbert modular forms.

4. $R = \mathbb{T}$ THEOREMS.

See for instance [FT], although this contains some shortcomings.

Suppose that F is a totally real field of even degree, that $l > 3$ is a prime unramified in F (so that in particular $[F(\zeta_l) : F] > 2$), and that S is a finite set of finite places of F not dividing l. Suppose also that

$$\overline{r} : G_F \longrightarrow GL_2(\overline{\mathbb{F}}_l)$$

is an absolutely irreducible continuous representation unramified outside l and S, with $\det \overline{r} = \overline{\epsilon}_l^{-1}$ and such that for $v \in S$ we have

$$\mathrm{tr}\, \overline{r}|_{\ker(I_{F_v} \twoheadrightarrow k(v)^\times)} \equiv 2,$$

while for all $v|l$ the restriction $\overline{r}|_{G_{F_v}}$ is Fontaine-Laffaille with Hodge-Tate numbers $\{0, 1\}$.

If R is a complete noetherian local $\mathbb{Z}_l$-algebra and if $r : G_F \to GL_2(R)$ lifts $\overline{r}$, then in the FL case we say that r is an *S-lift* (resp. *a narrow S-lift*) of $\overline{r}$ if

- $\det r = \epsilon_l^{-1}$;
- r is unramified outise S and l;
- if $v \in S$ then
$$\mathrm{tr}\, r|_{\ker(I_{F_v} \twoheadrightarrow k(v)^\times)} \equiv 2$$
(resp. if $v \in S$ then
$$\mathrm{tr}\, r|_{I_{F_v}} \equiv 2);$$
- if $v|l$ then $r|_{G_{F_v}}$ is Fontaine-Laffaille.

There is universal S-lift (resp, narrow S-lift)

$$r_S^{\mathrm{univ}} : G_F \longrightarrow GL_2(R_{S,\overline{r}}^{\mathrm{univ}})$$

(resp.

$$r_{-,S,}^{\mathrm{univ}} : G_F \longrightarrow GL_2(R_{S,\overline{r}}^{\mathrm{univ}}))$$

of $\overline{r}$.

Theorem 4.1. *Keep the above notation and assumptions. Suppose further that*

- *$\overline{r}$ is automorphic of level $U_0(S)$;*
- *$\overline{r}|_{G_{F(\zeta_l)}}$ is absolutely irreducible;*
- *if $v \in S$ then $\# k(v) \equiv 1 \bmod l$;*
- *if $v \in S$ then $\overline{r}|_{G_{F_v}} = 1$.*

Then $R_{-,S,\overline{r}}^{\mathrm{univ}}$ is a finite $\mathbb{Z}_l$-algebra; and if $L/\mathbb{Q}_l$ is a finite extension and

$$r : G_F \longrightarrow GL_2(\mathcal{O}_L)$$

is a narrow S-lift of $\overline{r}$, then r is automorphic of weight 2 and level $U_0(S)$.

Corollary 4.2. *Keep the above notation and assumptions. Suppose further that*

- *$\overline{r}$ is automorphic of level $U_1(S)$;*

- $\overline{r}|_{G_{F(\zeta_l)}}$ *is absolutely irreducible.*

Then $R^{\mathrm{univ}}_{S,\overline{r}}$ *is a finite* $\mathbb{Z}_l$*-algebra; and if* $L/\mathbb{Q}_l$ *is a finite extension and*

$$r : G_F \longrightarrow GL_2(\mathcal{O}_L)$$

is an S*-lift of* $\overline{r}$*, then* r *is automorphic of weight 2 and level* $U_1(S)$*.*

The corollaries follow from the theorems by the usual Skinner-Wiles argument (see [SW]) using theorem 3.1. We need the following result from class field theory:

Proposition 4.3. *Let* S *be a finite set of places of a number field* K *. For each* $v \in S$ *let* L'_v/K_v *be a finite Galois extension. Then there is a finite solvable Galois extension* L/K *such that if* $w|v \in S$*, then* $L_w \cong L'_v$ *as a* K_v*-algebra. Moreover, if* K^{avoid}/K *is any finite extension then we can choose* L *to be linearly disjoint from* K^{avoid}*.*

5. Residual potential modularity

Theorem 5.1. *Let K^{avoid}/K be a Galois extension of number fields. Suppose also that S is a finite set of places of K. For $v \in S$ let L'_v/K_v be a finite Galois extension. Suppose also that T/K is a smooth, geometrically connected curve and that for each $v \in S$ we are given a non-empty,* $\mathrm{Gal}\,(L'_v/K_v)$*-invariant, open subset $\Omega_v \subset T(L'_v)$. Then there is a finite Galois extension L/K and a point $P \in T(L)$ such that*

- *L/K is Galois and linearly disjoint from K^{avoid} over K;*
- *if $v \in S$ and w is a prime of L above v then L_w/K_v is isomorphic to L'_v/K_v and $P \in \Omega_v \subset T(L'_v) \cong T(L_w)$. (This makes sense as Ω_v is* $\mathrm{Gal}\,(L'_v/K_v)$*-invariant.)*

(See [MB].)

Lemma 5.2. *Suppose that l is an odd prime and that*

$$\overline{r} : G_{\mathbb{Q}_l} \longrightarrow GL_2(\mathbb{F}_l)$$

is Fontaine-Laffaille with Hodge-Tate numbers $\{0, -1\}$ and has $\det \overline{r} = \overline{\epsilon}_l$. Then there is a finite unramified extension $L/\mathbb{Q}_l$ and an elliptic curve E/L with good reduction such that

$$E[l] \cong \overline{r}|_{G_L}.$$

Proof: If $\overline{r}$ is irreducible take E to be any elliptic curve with good supersingular reduction and L sufficiently large.

If on the other hand $\overline{r}$ is reducible then there is a peu-ramifie extension

$$(0) \longrightarrow \overline{\epsilon}_l \overline{\chi}^{-1} \longrightarrow \overline{r} \longrightarrow \overline{\chi} \longrightarrow (0)$$

for some unramified character $\overline{\chi} : G_{\mathbb{Q}_l} \longrightarrow \mathbb{F}_l^{\times}$. Choose any ordinary elliptic curve $\overline{E}/\overline{\mathbb{F}}_l$. If L is sufficiently large then $\overline{\chi}|_{G_L}$ is trivial, $\overline{E}$ is defined over the residue field of L and G_L acts trivially on $\overline{E}[l](\overline{\mathbb{F}}_l)$. Denote by $\psi : G_L \to \mathbb{Z}_l^{\times}$ the unramified character by which G_L acts on $T_l\overline{E}$. (So that $\psi \bmod l = 1$.) By Serre-Tate theory, lifts of $\overline{E}$ to L are parametrized by $H^1(G_L, \mathbb{Z}_l(\epsilon_l \psi^2))$. On the other hand the extension $\overline{r}|_{G_L}$ gives an element in

$$\mathcal{O}_L^{\times}/(\mathcal{O}_L^{\times})^l \subset L^{\times}/(L^{\times})^l \cong H^1(G_L, \overline{\epsilon}_l).$$

What we need to show is that $\mathcal{O}_L^{\times}/(\mathcal{O}_L^{\times})^l$ is contained in the image of

$$H^1(G_L, \mathbb{Z}_l(\epsilon_l \psi^2)) \longrightarrow H^1(G_L, \overline{\epsilon}_l) \cong L^{\times}/(L^{\times})^l.$$

This is equivalent to the map

$$\mathcal{O}_L^{\times}/(\mathcal{O}_L^{\times})^l \longrightarrow H^1(G_L, \overline{\epsilon}_l) \longrightarrow H^2(G_L, \mathbb{Z}_l(\epsilon_l \psi^2))[l]$$

being trivial. After apply Tate duality this is, in turn, equivalent to the map

$$H^0(G_L, (\mathbb{Q}_l/Z_l)(\psi^{-2}))/l \longrightarrow \mathrm{Hom}\,(G_L, l^{-1}\mathbb{Z}_l/\mathbb{Z}_l) \longrightarrow \mathrm{Hom}\,(G_L, l^{-1}\mathbb{Z}_l/\mathbb{Z}_l)/\mathrm{Hom}_{\,\mathrm{nr}}(G_L, l^{-1}\mathbb{Z}_l/\mathbb{Z}_l)$$

being trivial, where $\mathrm{Hom}_{\mathrm{nr}}(G_L, \mathbb{F}_l)$ denotes the space of unramified homomorphisms. However $x \in H^0(G_L, (\mathbb{Q}_l/\mathbb{Z}_l)(\psi^{-2}))$ gets sent to

$$\sigma \longmapsto ((\psi(\sigma)^{-2} - 1)/l)x$$

which is unramified because ψ is.$\square$

Theorem 5.3. *Suppose that $l > 3$ is a prime, and*

$$\overline{r} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_l)$$

is a continuous representation satisfying:

- $\det \overline{r} = \overline{\epsilon}_l^{-1}$*;*
- $\mathrm{tr}\, \overline{r}(c) = 0$*, where c denotes any complex conjugation;*
- $\overline{r}$ *is unramified away from $2l$;*
- $\overline{r}|_{G_{\mathbb{Q}_l}}$ *is Fontaine-Laffaille with Hodge-Tate numbers $\{0, 1\}$;*
- $\overline{r}|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} = \overline{\chi} \oplus \overline{\chi\epsilon_l}^{-1}$ *for some unramified quadratic character $\overline{\chi}$ of $G_{\mathbb{Q}_2}$.*

Then there is an even degree finite totally real Galois extension $F/\mathbb{Q}$ unramified above l, which is linearly disjoint from $\overline{\mathbb{Q}}^{\ker \overline{r}}[\zeta_l]$ over $\mathbb{Q}$, such that $\overline{r}|_{G_F}$ is automorphic of weight 2 and level $U_1(S')$ for some set S' containing the primes above 2.

Proof: Sketch: Choose an imaginary quadratic field $M/\mathbb{Q}$ in which l is unramified but which ramifies at some rational prime bigger than 3. Let $p \equiv -1 \bmod l$ be a prime which splits in M. Choose a finite extension N/M and a continuous character

$$\theta : (\mathbb{A}_M)^\times \longrightarrow N^\times$$

such that

- $\theta|_{M^\times} : \alpha \to \alpha$,
- $\theta|_{\mathbb{A}^\times}(x) = ||x||^{-1} x_\infty \delta_{M/\mathbb{Q}}(x)$, where $\delta_{M/\mathbb{Q}}$ is the quadratic character corresponding to $M/\mathbb{Q}$,
- θ is unramified above l,
- θ is ramified of degree $p-1$ at one prime above p and unramified at the other.

To see that this is possible let $U = \mathbb{C}^\times \times \prod_{v \not| \infty} U_v$, where $U_v = \mathcal{O}_{M,v}^\times$, unless v is ramified above $\mathbb{Q}$, in which case $U_v = 1 + \varpi_v \mathcal{O}_{F,v}$. Then we can certainly define $\theta : \mathbb{A}^\times U \to N^\times$ satisfying the last three conditions. As long as $\theta|_{M^\times \cap \mathbb{A}^\times U} : \alpha \mapsto \alpha$, then we can extend θ first to $M^\times \mathbb{A}^\times U$ and then to $\mathbb{A}_M^\times$ with the desired properties. However, if $\alpha \in M^\times \cap \mathbb{A}^\times U$ then

$${}^c\alpha/\alpha \in \mathcal{O}_M^\times \cap U = \{\pm 1\} \cap U = \{1\},$$

so that $\alpha \in \mathbb{Q}^\times$ and

$$\theta(\alpha) = \mathrm{sgn}\,(\alpha) \prod_{v \not| \infty} |\alpha|_v^{-1} = \alpha.$$

Also choose an odd rational prime l' which splits completely in N at which θ and $\overline{r}$ are unramified, and a prime λ of N above l'. Then we have a character

$$\theta_\lambda : G_M^{\mathrm{ab}} \cong \mathbb{A}_M^\times/M^\times \longrightarrow \mathcal{O}_{N,\lambda}^\times \cong \mathbb{Z}_l^\times.$$

Write $\overline{\theta}_\lambda$ for its reduction. Note that $\det \operatorname{Ind}_{G_M}^{G_\mathbb{Q}} \theta_\lambda = \epsilon_l^{-1}$ and that $(\operatorname{Ind}_{G_M}^{G_\mathbb{Q}} \overline{\theta}|_\lambda)|_{G_{\mathbb{Q}(\zeta_{l'})}}$ is absolutely irreducible. (Look at what happens locally on $G_{\mathbb{Q}_p}$.)

Consider the moduli space T for elliptic curves E together with isomorphisms

$$E[l]^\vee \cong \overline{r}$$

and

$$E[l']^\vee \cong \operatorname{Ind}_{G_M}^{G_\mathbb{Q}} \overline{\theta}_\lambda$$

both sending the Weil-pairing to the determinant pairing. Then T is a geometrically connected curve over $\mathbb{Q}$. It follows from the previous lemma that there are finite unramified extensions $L_l'/\mathbb{Q}_l$ and $L_{l'}'/\mathbb{Q}_{l'}$ such that T has points over L_l' and $L_{l'}'$ with good reduction (i.e. integral j-invariant).

Set $F^{\mathrm{avoid}} = \overline{\mathbb{Q}}^{\ker(\overline{r} \times \operatorname{Ind}_{G_M}^{G_\mathbb{Q}} \overline{\theta}_\lambda)}(\zeta_{ll'})$. Let S_1 denote the primes that ramify in M or above which θ is ramified. Set $S = \{\infty, l, l'\} \cup S_1$. Set $K = \mathbb{Q}$, $L_\infty' = \mathbb{R}$, L_l' and $L_{l'}'$ as in the previous paragraph, and for $v \in S_1$ let L_v' be a finite Galois extension of $\mathbb{Q}_v$ such that $(\operatorname{Ind}_{G_M}^{G_\mathbb{Q}} \theta_\lambda)|_{G_{L_v'}}$ is unramified . Also set $\Omega_\infty = T(\mathbb{R})$, Ω_l to be the good reduction locus in $T(L_l')$, $\Omega_{l'}$ to be the good reduction locus in $T(L_{l'}')$ and for $v \in S_1$ set $\Omega_v = T(L_v')$. Applying theorem 5.1 we obtain a finite Galois totally real field $F/\mathbb{Q}$ linearly disjoint from F^{avoid} in which l and l' are unramified and an elliptic curve E/F such that

- $E[l]^\vee \cong \overline{r}|_{G_F}$ and $E[l']^\vee \cong \operatorname{Ind}_{G_{MF}}^{G_F} \overline{\theta}_\lambda|_{G_{MF}}$, which is unramified at all primes not dividing l';
- E has good reduction at l and l';
- MF/F is unramified at all finite primes.

Then it follows from theorem 3.2 that $E[l']^\vee$ is automorphic over F of weight 2 and level $U_0(\emptyset)$. Thus, by corollary 4.2, $T_{l'}E^\vee$ is automorphic over F of weight 2 and level $U_1(S')$ for some S', which we can take to contain the primes above 2. Thus $E[l]^\vee \cong \overline{r}|_{G_F}$ is automorphic over F of weight 2 and level $U_1(S')$ for some S', which contains the primes above 2. $\square$

6. Applications

Corollary 6.1. *Suppose that l is an odd prime, and*

$$r : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{Q}}_l)$$

is an irreducible continuous representation with reduction $\overline{r}$ satisfying:

- $\det r = \epsilon_l^{-1}$;
- $\operatorname{tr} r(c) = 0$, *where c denotes any complex conjugation;*
- *r is unramified away from $2l$;*
- *$r|_{G_{\mathbb{Q}_l}}$ is crystalline with Hodge-Tate numbers $\{0, 1\}$;*
- *$r|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} = \chi \oplus \chi\epsilon_l^{-1}$ for some unramified quadratic character χ of $G_{\mathbb{Q}_2}$;*
- *$\overline{r}$ factors through $GL_2(\mathbb{F}_l)$;*
- *$\overline{r}|_{G_{\mathbb{Q}(\zeta_l)}}$ is absolutely irereducible.*

Then there is a continuous representation

$$r' : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{Q}}_3)$$

and an isomorphism of fields $\iota : \overline{\mathbb{Q}}_l \xrightarrow{\sim} \overline{\mathbb{Q}}_3$ such that

- $\det r' = \epsilon_3^{-1}$,
- *r' is unramified outside* 6,
- *if $p \not| 6l$ then* $\operatorname{tr} r'(\mathrm{Frob}_p) = \iota(\operatorname{tr} r(\mathrm{Frob}_p))$,
- $r'|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} = \chi \oplus \chi\epsilon_3^{-1}$;
- *$r'|_{G_{\mathbb{Q}_3}}$ is crystralline with Hodge-Tate numbers $\{0, 1\}$.*

Proof: Sketch: If $l = 3$ there is nothing to prove, so assume $l > 3$. By theorem 5.3 and corollary 4.2, we see that $r|_{G_F}$ is automorphic over F of weight 2 and level $U_1(S')$. We then construct r' by the Brauer theorem argument in section 5.5 of [BLGGT]. $\square$

From this and theorem 1.2 we deduce that:

Corollary 6.2. *Suppose that l is an odd prime. Then there is no continuous representation and*

$$r : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{Q}}_l)$$

with reduction $\overline{r}$ satisfying:

- $\det r = \epsilon_l^{-1}$;
- $\operatorname{tr} r(c) = 0$, *where c denotes any complex conjugation;*
- *r is unramified away from $2l$;*
- *$r|_{G_{\mathbb{Q}_l}}$ is crystalline with Hodge-Tate numbers $\{0, 1\}$;*
- *$r|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} = \chi \oplus \chi\epsilon_l^{-1}$ for some unramified quadratic character χ of $G_{\mathbb{Q}_2}$;*
- *$\overline{r}$ factors through $GL_2(\mathbb{F}_l)$;*
- *$\overline{r}|_{G_{\mathbb{Q}(\zeta_l)}}$ is absolutely irereducible.*

Corollary 6.3. *Suppose that $l > 3$ is a prime, and*

$$\overline{r} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_l)$$

is a continuous representation satisfying:

- $\det \overline{r} = \overline{\epsilon}_l^{-1}$*;*
- $\operatorname{tr} \overline{r}(c) = 0$*, where c denotes any complex conjugation;*
- $\overline{r}|_{G_{\mathbb{Q}_l}}$ *is Fontaine-Laffaille with Hodge-Tate numbers $\{0, 1\}$;*
- $\overline{r}$ *is unramified away from $2l$;*
- $\overline{r}|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} = \overline{\chi} \oplus \overline{\chi\epsilon_l}^{-1}$ *for some unramified quadratic character $\overline{\chi}$ of $G_{\mathbb{Q}_2}$.*

Then $\overline{r}$ has a lift

$$r : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{Q}}_l)$$

such that

- $\det r = \epsilon_l^{-1}$,
- *r is unramified outside $2l$,*
- *$r|_{G_{\mathbb{Q}_l}}$ is crystalline with Hodge-Tate numbers $\{0, 1\}$,*
- *$r|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} \cong \chi \oplus \chi\epsilon_l^{-1}$ for some unramified quadratic character χ.*

Proof: Sketch: Look at the universal deformation ring R^{univ} for deformations of $\overline{r}$ of this sort. A Galois cohomology calculation shows it has Krull dimension ≥ 1. On the other hand it follows from theorems 5.3 and 4.2 and some simple algebra that this deformation ring is finite over $\mathbb{Z}_l$. Thus it has a characteristic $\overline{\mathbb{Q}}_l$ point, as desired.□

Corollary 6.4. *Suppose that $l > 3$ is a prime and that*

$$\overline{r} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_l)$$

is a continuous representation satisfying:

- $\det \overline{r} = \overline{\epsilon}_l^{-1}$*;*
- $\operatorname{tr} \overline{r}(c) = 0$*, where c denotes any complex conjugation;*
- $\overline{r}|_{G_{\mathbb{Q}_l}}$ *is Fontaine-Laffaille with Hodge-Tate numbers $\{0, 1\}$;*
- $\overline{r}$ *is unramified away from $2l$;*
- $\overline{r}|_{G_{\mathbb{Q}_2}}^{\mathrm{ss}} = \overline{\chi} \oplus \overline{\chi\epsilon_l}^{-1}$ *for some unramified quadratic character $\overline{\chi}$ of $G_{\mathbb{Q}_2}$.*

Then there is an extension

$$(0) \longrightarrow 1 \longrightarrow \overline{r} \longrightarrow \overline{\epsilon}_l^{-1} \longrightarrow (0).$$

Proof: Sketch: corollaries 6.3 and 6.2 immediatley imply that $\overline{r}|_{G_{\mathbb{Q}(\zeta_l)}}$ must be reducible. Thus there are two possibilities:

1) $\overline{r} = \operatorname{Ind}_{G_E}^{G_{\mathbb{Q}}} \overline{\theta}$, where E is the unique quadratic subfield of $\mathbb{Q}(\zeta_l)$ and $\overline{\theta}$ is some character, tamely ramified at l. Thus $\overline{r}(I_{E_l})$ consists of scalar matrices, and so $\overline{r}|_{I_{\mathbb{Q}_l}} = \overline{\chi}_1 \oplus \overline{\chi}_2$, where $(\overline{\chi}_1/\overline{\chi}_2)^2 = 1$. However either $\{\overline{\chi}_1, \overline{\chi}_2\} = \{\overline{\epsilon}_l^{-1}, 1\}$ or $\{\overline{\omega}_2^{-1}, \overline{\omega}_2^{-l}\}$. thus we must either have $\overline{\epsilon}_l^2 = 1$ or $\overline{\omega}_2^{l-1} = 1$. This would contradict $l > 3$.

2) $\overline{r}^{\mathrm{ss}} = \overline{\chi}_1 \oplus \overline{\chi}_2$. Then we see that $\{\overline{\chi}_1, \overline{\chi}_2\} = \{1, \overline{\epsilon}_l^{-1}\}$, as desired. Corollary 4.2 of [Sc] gives the desired result. $\square$

Theorem 6.5 (Mazur)**.** *If $l > 3$ is a prime number and $E/\mathbb{Q}$ is an elliptic curve with $\#E[2](\mathbb{Q}) = 4$, then E can not have a point oif exact order l.*

See [M].

Fermat's last theorem follows from this and corollary 6.4 as explained in sections 4.1 and 4.2 of [Se].

References

[BLGGT] T. Barnet-Lamb, T. Gee, D. Geraghty and R. Taylor, *Potential automorphy and change of weight*, Annals 179 (2014).

[F] J.-M. Fontaine, *Il n'y a pas de variete abelienne sur* $\mathbb{Z}$, Invent. Math. 81 (1985).

[FT] Notes by T. Feng of a course by R.Taylor on 'Automorphy Lifting' available at `https://math.berkeley.edu/~fengt/stanford_course.html`

[GM] M. Goresky and R. MacPherson, *The topological trace formula*, Crelle 560 (2003).

[M] B. Mazur, *Modular curves and the Eisenstein ideal*, Pub. Math. IHES 47 (1977).

[MB] L. Moret-Bailly, *Groupes de Picard et problemes de Skolem II*, Ann. Scient. ENS 22 (1989).

[Sc] R. Schoof, *Abelian varieties over* $\mathbb{Q}$ *with bad reduction in one prime only*, Comp. Math. 141 (2005).

[Se] J.-P. Serre, *Sur les representations modulaires de degre 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987).

[SW] C. Skinner and A. Wiles, *Base change and a problem of Serre*, Duke Math. J. 107 (2001).

[T] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. 98 (1989).