The Role of Ribet's Theorem in Wile's Proof of FLT

Cooper Young

June 3rd, 2022

Abstract

In this expository paper, we show how Ribet's theorem applies to Frey curves and how, with the Modularity Theorem, the proof of Fermat's Last Theorem was attained. We follow the original paper [6], though I've supplied additional commentary and reorganized some of the results.

Contents

1 Introduction

The Fermat curve F_n is defined to be the complex set of solutions to

$$x^n + y^n = z^n$$

for $n \geq 2$. Each F_n is a non-singular plane projective curve, and since the homogeneous polynomial that defines it has degree n, the genus-degree formula (proved in the last problem set) tells us that the genus of F_n is $\frac{1}{2}(d-1)(d-2)$. In 1975, Yves Hellegouarch became one of the first mathematicians to think of associating rational points on F_n with elliptic curves. Specifically, given a solution $a^n + b^n = c^n$, Hellegouarch defined the curve $y^2 = x(x - a^n)(x + b^n)$. Gerheard Frey studied these curves, which soon became known as Frey Curves, and drew attention to unusual properties that they have.

Let E be an elliptic curve defined over a field K of characteristic zero, and let $\bar{K}$ be the algebraic closure of K. Let $l \geq 5$ be prime and recall that the l^n-torsion points of E over $\bar{K}$, denoted $E(\bar{K})[l^n]$, is isomorphic to $(\mathbb{Z}/l^n\mathbb{Z})^2$. The absolute galois group $G_K := \mathrm{Gal}(\bar{K}/K)$ acts on $E(\bar{K})[l^n]$ by transforming the coordinates of points. Notice that the image of this transformation still lies in $E(\bar{K})[l^n]$ since E is defined over K so any element in the absolute galois group leaves the equation of E fixed. We have a natural chain of projections $E(\bar{K})[l^{n+1}] \to E(\bar{K})[l^n]$ which allows us to define the Tate module, $T_l(E) := \varprojlim E(\bar{K})[l^n]$, which G_K still acts on. From its construction, we see that $T_l(E) \cong \mathbb{Z}_l^2$, and hence we have a Galois representation $\rho_{E,l} : G_K \to \mathrm{GL}_2(\mathbb{Z}_l) \subset \mathrm{GL}_2(\mathbb{Q}_l)$ which can be shown to be continuous. Note that from our discussion above, we also have the associated representations $\bar{\rho}_{E,l^n} : G_K \to \mathrm{Aut}\left(E(\bar{K})[l^n]\right) \cong \mathrm{GL}_2(\mathbb{F}_{l^n})$ which can be realized as $\bar{\rho}_{E,l^n} \cong \rho_{E,l} \pmod{l^n}$.

2 The Setup for Ribet

Now that we have our definitions out of the way, we can start working with them. From now on, we let E be a Frey curve, unless specified otherwise. The discriminant for a general elliptic curve of the form $y^2 = x^3 + Ax^2 + Bx$ is $\Delta = (AB)^2 - 4B^3$. Hence for our Frey curve E, we can use the fact that $a^n + b^n = c^n$ to show

$$\Delta(E) = (b^n - a^n)^2(-a^n b^n)^2 - 4(-a^n b^n)^3 = (abc)^{2n}$$

It turns out that this is not the minimal discriminant, but with some simple change of variables we get a minimal discriminant of

$$\Delta_{\min}(E) = 2^{-8}(abc)^{2n}$$

For any prime p, we can take E and consider its reduction to a curve $\tilde{E}$ over $\mathbb{F}_p$. If $\tilde{E}$ is still an elliptic curve, then we say that E has good reduction at p and otherwise it has bad reduction. We say that an elliptic curve is semi-stable if for any prime p of bad reduction, only two roots become congruent modulo p. Since a, b, and c are coprime and E has bad reduction precisely at the primes dividing abc, we get that Frey curves are semi-stable.

We now prove various propositions which will allow us to apply Ribet's main theorem to Frey curves. Specifically, we first show that $\bar{\rho}_{E,l}$ (defined in the introduction) is irreducible and finite at every odd prime.

Proposition 1 ([7] Proposition 6): The representation $\bar{\rho}_{E,l}$ is an irreducible two-dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Proof: This result was first realized by Mazur in [5], though Serre gave a simple proof in [7]. Here we follow Serre's argument, modified slightly with ideas from this proposition's proof in [2].

Seeking a contradiction, suppose that $\bar{\rho}_{E,l}$ is reducible. Then E contains a subgroup X of order l that is rational over $\mathbb{Q}$. Since E is semi-stable and satisfies $E(\mathbb{Q})[2] \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^2$ (since E splits completely over $\mathbb{Q}$), the existence of X implies that we can find an isogenous elliptic curve E' which has a rational point of order l and also satisfies $|E'(\mathbb{Q})[2]| = 4$. This implies that $E'(\mathbb{Q})_{\text{tors}} \geq 4l$, but by Mazur's Theorem there are finitely many possibilities for the torsion subgroup of $E'(\mathbb{Q})$ and the largest of which only has cardinality 16, so for $l \geq 5$ we have a contradiction.

□

Let p be prime and choose a place v in $\bar{\mathbb{Q}}$ lying over p. The decomposition group D_v can be identified as $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ where $\bar{\mathbb{Q}}_p$ is the algebraic closure of $\mathbb{Q}_p$. Let I_v be the inertia subgroup of D_v and recall that D_v/I_v is isomorphic to the pro-cyclic group $\hat{\mathbb{Z}}$ generated by the Frobenius map $x \mapsto x^p$ (note that specifically it is a topological generator with the Krull topology on our group). We can lift this generator back to D_v and obtain an element denoted $Frob_v$, which is well defined modulo I_v.

We say that the representation ρ is unramified at p if $\rho(I_v) = \{1\}$. A different place v' above p takes the form $v' = \sigma v$ for some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and from the definitions of decomposition and inertia groups, we see that $D_{v'}$ and $I_{v'}$ are conjugate to D_v and I_v, respectively. Therefore, being unramified at p is independent of our choice of v. If ρ is unramified at p, notice that $\rho(Frob_v)$ is independent of our choice in lifting and hence is well-defined.

Given an integer k, we define the valuation of k at p, denoted $v_p(k)$, to be the exponent of the highest power of p which divides k. We are now ready for the next two propositions.

Proposition 2: Let E be an elliptic curve of the form $y^2 = x(x-A)(x+B)$ for A, B non-zero relatively prime integers with $A+B$ non-zero. If $p \neq l$, then $\bar{\rho}_{E,l}$ is unramified at p if and only if $v_p(\Delta_{\min}) \equiv 0 \pmod{l}$.

Sketch proof: Here I've combined two results from Ribet's paper into one. To prove this statement, one first shows that if $p \neq l$ and $p|N$ (where N is the conductor of E) then $\bar{\rho}_{E,l}$ is unramified at p if and only if $v_p(\Delta_{\min}) \equiv 0 \pmod{l}$. This is Proposition 3.4 in [6], though the proof redirects the reader to [3]. The details are omitted here since it is a consequence of the theory of Tate curves, which I don't have time to go into.

We now want to strip away the condition that $p|N$. If p and N are coprime, then E has good reduction at p and as a consequence is $\bar{\rho}_{E,l}$ is unramified at p (this is part of Proposition 3.3 in [6] whose proof can be found in [7]). Furthermore, $(p, N) = 1$ implies that $v_p(\Delta_{\min}) = 0$ and hence $v_p(\Delta_{\min}) \equiv 0 \pmod{l}$ is satisfied.

□

Note that Proposition 3.3 in [6] also claims that for each v dividng p, we have the congruence $\mathrm{Tr}\left(\rho(Frob_v)\right) \equiv p + 1 - |\tilde{E}(\mathbb{F}_p)| \pmod{l}$, but we won't need this result for the purposes of this paper. Now, all that's left for us to do is address the case when $p = l$, and to do so we need to introduce the notion of finiteness.

Let p be prime and v be a place above it. By restricting the action of $G_{\mathbb{Q}}$ on $E[l]$ to the decomposition group D_v, we may view $E[l]$ as a $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-module. We say that the representation ρ is finite at p if there is a finite flat group scheme $\mathcal{V}$ of type (l, l) over $\mathbb{Z}_p$ such that $\mathcal{V}(\bar{\mathbb{Q}}_p)$ and $E[l]$ are isomorphic as $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q})$-modules. It can be shown that when $p \neq l$, finiteness at p implies that ρ is unramified at p.

Proposition 3 ([6] Proposition 3.5): The representation $\bar{\rho}_{E,l}$ is finite at a prime number p if and only if $v_p(\Delta_{\min}) \equiv 0 \pmod{l}$.

For a proof of this proposition, Ribet directs the reader to [7] page 201, though I could not find an explanation for this statement there. Note that the only additional information that this proposition gives us is finiteness for the case $p = l$, but this allows us to fully utilize Ribet's Theorem in the next section.

3 Ribet's Theorem and Implications

We start off with the main theorem of Ribet's 1990 paper:

Ribet's Theorem ([6] Theorem 5.1): Let ρ be an irreducible two-dimensional representation of $G_{\mathbb{Q}}$ over a finite field of characteristic $l > 2$. Assume that ρ is modular of square free level N, and that there is a prime $q|N$ where $q \neq l$ and at which ρ is not finite. Finally, suppose that p is a divisor of N at which ρ is finite. Then ρ is modular of level N/p.

The proof of this theorem is omitted since it is above the scope of this paper. However, we have the following corollary.

Corollary 1: The Modularity Theorem for semi-stable elliptic curves implies Fermat's Last Theorem.

Proof: Note that if there is an integral point (a, b, c) on F_n where $n = rs$, then (a^r, b^r, c^r) is a solution to F_s. Hence to prove Fermat's Last Theorem, it suffices to show there are no integer points on F_l where l is prime. For the remainder of this proof, we fix l and let E denote the Frey curve associated to F_l.

Recall that from Proposition 1, we know that $\bar{\rho}_{E,l}$ is indeed a two-dimensional irreducible representation of $G_{\mathbb{Q}}$ over $\mathbb{F}_p$. We also know that $\Delta_{\min}(E) = 2^{-8}(abc)^{2l}$, so for any prime $p > 2$ we have $v_p(\Delta_{\min}) \equiv 0 \pmod{l}$, and therefore Proposition 3 implies that $\bar{\rho}_{E,l}$ is finite at every odd prime.

An equivalent definition of semi-stable elliptic curves is that the conductor N of E is square free. Since the conductor of an elliptic curves is an integer divisible precisely at the primes where E has bad reduction, we have

$$N = \prod_{p|(abc)} p$$

where our product ranges over primes. Note that to satisfy $a^l + b^l = c^l$, exactly two of the integers must be odd and the other must be even. We now know that $2|N$ but $\bar{\rho}_{E,l}$ is not finite at 2. If the Modularity Theorem is true for semi-stable elliptic curves, then $\bar{\rho}_{E,l}$ is modular and we can find a weight two newform f of level N.

We can now employ Ribet's Theorem to get a weight two newform of level $\frac{N}{p}$ for any odd prime $p|N$. In fact, we can inductively apply Ribet's Theorem to eventually get a a weight two newform g of level 2. Let $S_2(\Gamma_0(M))$ denote the space of weight 2 cusp forms of $\Gamma_0(M)$. There are many ways to compute the dimension of $S_2(\Gamma_0(M))$ (see [1] for instance), and it can be shown that $\dim\big(S_2(\Gamma_0(2))\big) = 0$. Therefore, such a g cannot exist and so we have proven Fermat's Last Theorem.

□

References

[1] Diamond, Fred and Jerry Shurman. *A First Course in Modular Forms.* Springer, New York, 2005.

[2] Darmon, Henri, Fred Diamond, Richard Taylor. *Fermat's Last Theorem* (2007).

[3] Frey, Gerhard. *Links between stable elliptic curves and certain diophantine equations.* Annales Universitatis Saraviensis 1, 1–40 (1986).

[4] Google Translate, Google. https://translate.google.com.

[5] Mazur, Barry. *Rational isogenies of prime degrees.* Invetiones Mathematicae 44, 129–162 (1978).

[6] Ribet, Kenneth. *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Annales de la Facult des Sciences de Toulouse (5) 11, no. 1, 116–139 (1990).

[7] Serre, Jean-Pierre. *Sur les reprsentations modulaires de degr 2 de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematics Journal 54, 179–230 (1987).