Canad. J. Math. Vol. **64** (2), 2012 pp. 282–300
http://dx.doi.org/10.4153/CJM-2011-059-8

Level Lowering Modulo Prime Powers and Twisted Fermat Equations

Sander R. Dahmen and Soroosh Yazdani

Abstract. We discuss a clean level lowering theorem modulo prime powers for weight 2 cusp forms. Furthermore, we illustrate how this can be used to completely solve certain twisted Fermat equations $ax^n + by^n + cz^n = 0$.

1 Introduction

Since the epoch making proof of Fermat's Last Theorem (FLT) [14, 15], many Diophantine problems have been resolved using the deep methods developed for FLT and extensions thereof. Among the basic tools involved are so-called level lowering results; see *e.g.,* [8, 9]. These provide congruences between modular forms of different levels. Until now, all applications of the modular machinery to Diophantine equations only involved level lowering modulo primes. Although a level lowering result modulo prime powers has recently been established [4], the statements there are not very fit for applications to Diophantine equations. The purposes of this paper are twofold. First, we give a clean level lowering result modulo prime powers that is suitable for applications to Diophantine equations. Second, we illustrate how this result can be applied by completely solving certain twisted Fermat equations, *i.e.,* Diophantine equations of the form

$$ax^n + by^n + cz^n = 0 \quad x, y, z, n \in \mathbb{Z},\ xyz \neq 0,\ n > 1,$$

where a, b, c are nonzero integers. For the twisted Fermat equations we consider, the genus one curve defined by $ax^3+by^3+cz^3 = 0$ has infinitely many rational points, the curve defined by $ax^9+by^9+cz^9 = 0$ has points everywhere locally, and level lowering modulo 3 also does not give enough information to deal with the exponent $n = 9$ case. The main application of our level lowering modulo prime powers theorem is then to use level lowering modulo 9 to deal with the exponent $n = 9$ case.

The organization of this paper is as follows. In Section 2 the level lowering result (Theorem 2.3) is stated and proved. In Section 3 we mainly deal with some issues related to irreducibility of mod 3 representations. In Section 4 we solve some twisted Fermat equations using level lowering modulo primes and level lowering modulo 9. Finally, in Section 5 we quickly discuss other possible methods to attack the twisted Fermat equation for exponent $n = 9$, and we prove that standard level lowering modulo 3 methods can never work for our examples.

Received by the editors September 1, 2010.
Published electronically September 15, 2011.
AMS subject classification: **11D41**, 11F33, 11F11, 11F80, 11G05.
Keywords: modular forms, level lowering, Diophantine equations.

2 Level Lowering Modulo Prime Powers

Let N be a positive integer and $S_2(\Gamma_0(N))$ denote the space of cuspidal modular forms of weight 2 with respect to $\Gamma_0(N)$. For any Hecke eigenform $f \in S_2(\Gamma_0(N))$, denote by K_f the field of definition of the Fourier coefficients of f, and by $\mathcal{O}_f$ its ring of integers. Note that the image of f under different embeddings of $K_f \to \mathbb{C}$ gives conjugate Hecke eigenforms in $S_2(\Gamma_0(N))$. As such, treating K_f as an abstract number field and f as a modular form with Fourier coefficients in K_f is akin to looking at f and all its Galois conjugates at the same time. We say that f is a *newform class* of weight 2 and level N if $f \in K[[q]]$ for a number field K, and the image of f under each (equiv. under any) embedding of $K \to \mathbb{C}$ is a normalized Hecke newform in $S_2(\Gamma_0(N))$. We usually omit the weight of the modular forms in this paper, since we are only working with weight 2 forms. The *degree* of the newform class f is the degree of the number field K_f. Denote by $G_{\mathbb{Q}}$ the absolute Galois group of $\mathbb{Q}$. Let f be a newform class of level N. Given a prime $\lambda \subset \mathcal{O}_f$ lying above l, we can construct (see, for example, [13]) a Galois representation

$$\rho_{\lambda^r}^f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_f/\lambda^r)$$

for which

- $\rho_{\lambda^r}^f$ is unramified away from Nl;
- $\mathrm{trace}(\rho_{\lambda^r}^f(\mathrm{Frob}_p)) \equiv a_p(f) \pmod{\lambda^r}$ and $\mathrm{Norm}(\rho_{\lambda^r}^f(\mathrm{Frob}_p)) \equiv p \pmod{\lambda^r}$ for all primes $p \nmid Nl$.

We remark that when ρ_{λ}^f is absolutely irreducible, $\rho_{\lambda^r}^f$ is uniquely determined (up to change of basis) for all positive integers r by the congruences above.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and minimal discriminant Δ. Let

$$\rho_{l^r}^E \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/l^r\mathbb{Z})$$

be the Galois representation coming from the natural Galois action of $G_{\mathbb{Q}}$ on $E[l^r](\overline{\mathbb{Q}})$. Assume that $N = N_0 M$ with $N_0, M \in \mathbb{Z}_{>0}$ and that there is an odd prime l such that the following hold:

- N_0 and M are coprime;
- M is square free;
- for all primes $p|M$ we have $l|v_p(\Delta)$;
- $E[l]$ is irreducible (*i.e.*, ρ_l^E is an irreducible Galois representation).

Then by Ribet's level lowering ([8,9]) there is a newform class of level N_0 and prime $\lambda \subset \mathcal{O}_f$ lying above l such that $\rho_l^E \simeq \rho_{\lambda}^f$ as Galois representations, or equivalently, that $a_p(E) \equiv a_p(f) \pmod{\lambda}$ for all primes $p \nmid N_0 l$.

Remark 2.1 Let $\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ be an irreducible Galois representation coming from a modular form of weight 2 that is semistable at l, with R a Noetherian complete local ring with the maximal ideal $\mathfrak{m}$ and $R/\mathfrak{m}$ of characteristic l. As usual, define

$$N(\rho) = \begin{cases} N_\rho & \text{if } \rho \text{ is flat at } l, \\ N_\rho l & \text{if } \rho \text{ is Selmer but not flat at } l, \end{cases}$$

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

where N_ρ is the prime to l Artin conductor of ρ (see [15] for the definitions of Selmer and flat). Then, Ribet's level lowering states that if R is a finite field, then there is a newform class of level $N(\rho)$ and prime $\lambda \subset \mathcal{O}_f$ such that $\rho_l^E \simeq \rho_\lambda^f$.

It is natural to ask what happens when $l^r | v_p(\Delta)$ for all $p|M$ (see [2]). The situation in this case is more complicated. We first need to assume that $E[l]$ is *strongly irreducible* to get around some technical issues with deformation theory.

Definition 2.2 We say a 2-dimensional Galois representation ρ of $G_{\mathbb{Q}}$ is *strongly irreducible*, if $\rho|_{G_{\mathbb{Q}(\sqrt{l^*})}}$ is absolutely irreducible for $l^* = (-1)^{(l-1)/2} l$.

As noted in [4], using results of [10], when $l \geq 5$ and E is semistable at l, then ρ_l^E is strongly irreducible if it is irreducible. We will deal with the case $l = 3$ for elliptic curves with full rational 2-torsion in Section 3.

We also need to assume that there is a unique newform class f and an unramified prime ideal λ at level N_0 to get the desired level lowering results.

Theorem 2.3 *Let $E/\mathbb{Q}$, N_0, M, l be as above. Assume that*

- *there is a positive integer r such that for all primes $p|M$ we have $l^r | v_p(\Delta)$;*
- *for all primes $p|N_0$ we have $l \nmid v_p(\Delta)$;*
- *$l^2 \nmid N$;*
- *$E[l]$ is strongly irreducible;*
- *there is a unique pair (f, λ) with f a newform class of level N_0 and $\lambda \subset \mathcal{O}_f$ an unramified prime lying above l such that $\rho_l^E \simeq \rho_\lambda^f$.*

Then $\rho_{l^r}^E \simeq \rho_{\lambda^r}^f$. In particular, if all of the above assumptions are satisfied, then

(i) *for all primes p with $p \nmid lN$,*

$$a_p(f) \equiv a_p(E) \pmod{\lambda^r};$$

(ii) *for all primes p with $p \nmid N_0 l$ and $p|N$,*

$$a_p(f) \equiv a_p(E)(1+p) \equiv \pm(1+p) \pmod{\lambda^r}.$$

Remark 2.4 Let us explain the reason for the assumptions made in this theorem. We need to assume $l^2 \nmid N$, since the $R = \mathbb{T}$ results in this situation are not strong enough for our applications. The assumption that λ is unramified is part of the uniqueness, in the sense that if λ is ramified, then there are two Hecke eigenforms f_1 and f_2 in the same conjugacy class that are congruent to each other. Finally, we are assuming that $l \nmid v_p(\Delta)$ for $p|N_0$. We make this assumption because we want to guarantee that $N(\rho_l^E) = N_0$ and not something smaller. This way, we do not have to deal with oldforms for our analysis.

Remark 2.5 A similar theorem using similar techniques is proved in [4], although the statements of the main result there (specialized to our case) assume that M is prime, N is square free, and $l \nmid N$. None of these assumptions is necessary for the main proof, and in fact for applications to Diophantine equations these assumptions are usually not fulfilled.

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

We will present the proof of Theorem 2.3 for completeness. The proof uses standard Taylor–Wiles machinery ([14, 15], see also [3]) relating the deformation ring of modular Galois representations to a particular Hecke algebra. Specifically, let f be a newform class of level N_0, and let $\lambda \subset \mathcal{O}_f$ be a prime lying above $l > 2$. Recall that a lifting of ρ_λ^f is a representation $\rho\colon \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(R)$, where R is a Noetherian complete local ring with the maximal ideal $\mathfrak{m}$ and the residue field $R/\mathfrak{m} = \mathcal{O}_f/\lambda$ such that $\rho \equiv \rho_\lambda^f \pmod{\mathfrak{m}}$. A deformation of ρ_λ^f is an equivalence class of such lifts. We say that ρ is a *minimal deformation* of ρ_λ^f, if the ramification types of ρ and ρ_λ^f are the same at all primes p. In particular at l, if ρ_λ^f is flat (when $l \nmid N_0$), then ρ is flat, and if ρ_λ^f is Selmer but not flat (when $l \,\|\, N_0$), then ρ is Selmer but not flat. In either case, we have $N(\rho) = N(\rho_\lambda^f) = N_0$.

Assume that ρ_λ^f is strongly irreducible and semistable at l. Then we know that there is a universal deformation ring R^{univ} and a universal deformation $\rho^{\mathrm{univ}}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R^{\mathrm{univ}})$ such that every minimal deformation ρ_λ^f is strictly equivalent to a unique specialization of ρ^{univ} under a unique homomorphism $R^{\mathrm{univ}} \to R$. Let $\mathbb{T}$ be the Hecke algebra acting on $S_2(\Gamma_0(N_0))$, completed at the maximal ideal corresponding to ρ_λ^f. If we assume that $N_0 = N(\rho_\lambda^f)$, then we have a surjective map $\Phi\colon R^{\mathrm{univ}} \to \mathbb{T}$. We have the following celebrated result.

Theorem 2.6 (Taylor–Wiles) *Let l be an odd prime. Assume that ρ_λ^f is strongly irreducible. Then $\Phi\colon R^{\mathrm{univ}} \to \mathbb{T}$ is an isomorphism and R^{univ} is a complete intersection.*

Proof For a proof when ρ_λ^f is assumed to be semistable, see [1, 14, 15]. To prove the result stated here we also need Diamond's strengthening [3]. We remark that in all of the above theorems, the statement proved is presented as $R_Q = \mathbb{T}_Q$, where R_Q is a universal deformation ring for certain non-minimal deformations and $\mathbb{T}_Q$ is the completed Hecke algebra acting on $S_2(\Gamma_Q)$. The case that we are using is when Q is the empty set. In this case $R_\varnothing = R$, however the group $\Gamma_\varnothing$ in the *loc. cit.* lies between $\Gamma_0(N)$ and $\Gamma_1(N)$. Fortunately this group is chosen in such a way that the space on which the diamond operator is acting trivially modulo l, is precisely $\Gamma_0(N)$. Therefore $\mathbb{T}_\varnothing = \mathbb{T}$. ∎

As pointed out in [4], $R = \mathbb{T}$ results are the key to proving level lowering statements.

Proposition 2.7 *Let g be a newform class of level N_g and degree 1. Assume that there is a pair (f, λ) with f a newform class of level N_f and $\lambda \subset \mathcal{O}_f$ an unramified prime lying above l, and a positive integer r such that*

- $N(\rho_l^g) = N(\rho_{l^r}^g) = N_f$;
- $\rho_\lambda^f \simeq \rho_l^g$;
- *there is no other pair (f', λ') with f' a newform class of level N_f and $\lambda' \subset \mathcal{O}_{f'}$ a prime lying above l such that $\rho_{\lambda'}^{f'} \simeq \rho_l^g$;*
- *ρ_l^g is strongly irreducible.*

Then $\rho_{l^r}^g \simeq \rho_{\lambda^r}^f$.

Proof Let R^{univ} be the universal deformation ring for the minimal deformations of ρ_λ^f. By results of [14] we get that $R^{\mathrm{univ}} = \mathbb{T}$. Since we are assuming that g has

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

rational integral coefficients and that $\rho_\lambda^f \simeq \rho_l^g$, we get that $\mathcal{O}_f/\lambda = \mathbb{Z}/l = \mathbb{F}_l$. Since we are also assuming that there is a unique (f, λ) and that λ is unramified, we get $\mathbb{T} = \mathcal{O}_{f,\lambda} = \mathbb{Z}_l$. Furthermore, we have that $N(\rho_{l^r}^g) = N_f$, therefore we get that $\rho_{l^r}^g$ is a minimal deformation of ρ_λ^f, hence it corresponds to a map $\mathbb{T} \to \mathbb{Z}/l^r$. However, there exists only one reduction map from $\mathbb{Z}_l$ to $\mathbb{Z}/l^r$, therefore $\rho_{l^r}^g$ is isomorphic to $\rho_{\lambda^r}^f$. ■

Remark 2.8 In Proposition 2.7, we are assuming that g is of degree 1 to simplify the notation and the proof and because it is the case we care most about in this paper. However, the proof does extend to the general case with some care.

We now give the proof of Theorem 2.3.

Proof Let $E/\mathbb{Q}$, N_0, M, and l be as required. In particular, assume that $E[l]$ is strongly irreducible. Since we are assuming that $l^r | v_p(\Delta)$ for all $p|M$ (and $l \nmid v_p(\Delta)$ for all $l|N_0$), we get that $N(\rho_{l^r}^E) = N_0$. By Ribet's level lowering we get that there is a newform class f of level N_0 and a prime λ such that $\rho_\lambda^f \simeq \rho_l^E$. Therefore, we can apply Proposition 2.7 to prove that $\rho_{l^r}^E \simeq \rho_{\lambda^r}^f$. As is well known, the congruences (i) and (ii) in the statement of the theorem follow by comparing the traces of Frobenius. ■

Remark 2.9 When f is not unique, all hope is not lost, and in favourable conditions, we can in fact get some explicit level lowering results. As an example, consider an elliptic curve $E/\mathbb{Q}$ of conductor $71M$ and minimal discriminant $71M^{27}$ for some square free positive integer M coprime to 71. Furthermore, assume that $E[3]$ is strongly irreducible. Such an elliptic curve certainly exists; for example, when $M = 2$, we have the elliptic curve $142e1$ in the Cremona database

$$E : y^2 + xy = x^3 - x^2 - 2626x + 52244.$$

By Ribet's level lowering, we can find a newform class f of level 71 and a prime $\lambda \subset \mathcal{O}_f$ lying above 3 such that $\rho_3^E \simeq \rho_\lambda^f$. There are two newform classes f_1 and f_2, each of degree 3, whose complex embeddings span all of $S_2(\Gamma_0(71))$. For $i = 1, 2$, we can check that $3\mathcal{O}_{f_i} = \lambda_{i,1}\lambda_{i,2}$, where $\lambda_{i,1}$ is of inertia degree one, while $\lambda_{i,2}$ is of inertia degree 2. The image of $\rho_{\lambda_{i,2}}^{f_i}$ is not contained in $\mathrm{GL}_2(\mathbb{F}_3)$, therefore $\rho_{\lambda_{i,2}}^{f_i} \not\simeq \rho_3^E$. By computing some Fourier coefficients, we get that $\rho_{\lambda_{1,1}}^{f_1} \simeq \rho_{\lambda_{2,1}}^{f_2}$. We conclude that ρ_l^E is isomorphic to both of these representations. Therefore, all the conditions of our level lowering result are fulfilled, except for the uniqueness of (f, λ). This prevents us from proving a level lowering result modulo 27. However, by studying the deformation ring explicitly, we can still prove a level lowering result modulo 9 in the following way. For $i = 1, 2$, we compute that $\mathcal{O}_{f_i}$ is generated by $a_5(f_i)$, explicitly

$$\mathcal{O}_{f_1} = \mathbb{Z}[t]/\langle t^3 - 5t^2 - 2t + 25\rangle,$$
$$\mathcal{O}_{f_2} = \mathbb{Z}[t]/\langle t^3 + 3t^2 - 2t - 7\rangle.$$

Furthermore, the full Hecke algebra acting on $S_2(\Gamma_0(71))$ has the representation

$$\mathbb{Z}[t]/\left\langle (t^3 - 5t^2 - 2t + 25)(t^3 + 3t^2 - 2t - 7)\right\rangle,$$

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

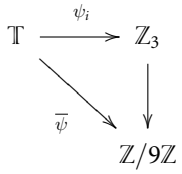
where $t = T_5$ is the fifth Hecke operator. Therefore, the universal deformation ring of ρ_3^E, which is the localization of the Hecke algebra at $\lambda_{i,1}$, is

$$\mathbb{T} = \mathbb{Z}_3[t]/\langle (t-\alpha_1)(t-\alpha_2)\rangle,$$

where $\alpha_1 \equiv 20 \pmod{27}$ and $\alpha_2 \equiv 11 \pmod{27}$. Notice that $\alpha_1 \equiv \alpha_2 \equiv 2 \pmod 9$, which means $\rho_{\lambda_{1,1}^2}^{f_1} \simeq \rho_{\lambda_{2,1}^2}^{f_2}$, a result that can also be read off from the Fourier coefficients of f_1 and f_2. Since ρ_{27}^E is unramified away from 3 and 71, and it is flat at 3, we have that ρ_{27}^E is a minimal deformation of ρ_3^E, hence it corresponds to a unique map $R^{\text{univ}} \to \mathbb{Z}/27\mathbb{Z}$. Note that this gives us two possible maps

$$\psi_i \colon \mathbb{T} \to \mathbb{Z}_3,$$
$$t \mapsto \alpha_i$$

corresponding to the two modular forms with coefficients in $\mathbb{Z}_3$. Let $\psi\colon \mathbb{T} \to \mathbb{Z}/27\mathbb{Z}$ correspond to ρ_{27}^E. Note that ψ is uniquely defined by the image of t, and there are three possible choices for this image: 2, 11, or 20. Reducing ψ modulo 9 we get that $\overline{\psi}\colon \mathbb{T} \to \mathbb{Z}/9\mathbb{Z}$ is given by $\overline{\psi}(t) = 2$. Furthermore, $\overline{\psi}$ corresponds to ρ_9^E, so we get the following commutative diagram.



By universality, the map $\mathbb{T} \xrightarrow{\psi_i} \mathbb{Z}_3 \to \mathbb{Z}/9\mathbb{Z}$ corresponds to the reduction of the λ_i-adic representation of f_i modulo λ_i^2, that is $\rho_{\lambda_i^2}^{f_i}$. Since this is the same as $\overline{\psi}$, which corresponds to ρ_9^E, we get that $\rho_9^E \simeq \rho_{\lambda_i^2}^{f_i}$ for $i = 1$ and 2.

In case we take for E the elliptic curve 142*e*1, we can check explicitly that $\rho_{27}^E \not\simeq \rho_{\lambda_{i,1}^3}^{f_i}$ for $i = 1$ or 2, since $a_5(E) = 2$, while $a_5(f_i) \equiv \alpha_i \not\equiv 2 \pmod{\lambda_{i,1}^3}$. The congruence modulo 9 can be verified by computing some Fourier coefficients explicitly.

3 Irreducibility mod 3

In this section, we obtain a criterion for proving that ρ_3^E is strongly irreducible when $E/\mathbb{Q}$ has a full rational 2-torsion structure. We start with a simple lemma.

Lemma 3.1 *Let $E/\mathbb{Q}$ be an elliptic curve. If ρ_3^E is irreducible but not strongly irreducible, then $\rho_3^E(G_{\mathbb{Q}})$ is contained in the normalizer of a split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_3)$.

Proof A (short) proof can be found in [11, Proposition 6]. ∎

Next we have a lemma that restricts the possibility of the image of a mod-3 Galois representation attached to an elliptic curve over $\mathbb{Q}$ with full rational 2-torsion.

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

Lemma 3.2 *Let $E/\mathbb{Q}$ be an elliptic curve with full rational 2-torsion. Then $\rho_3^E(G_{\mathbb{Q}})$ is not contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$.*

Proof Consider the modular curves $X_{\mathrm{split}}(3), X(2), X(1)$ and denote by j_2 and $j_{\mathrm{split},3}$ the j-maps from $X(2)$ to $X(1)$ and $X_{\mathrm{split}}(3)$ to $X(1)$ respectively. We have explicitly

$$j_2(s) = 2^8 \frac{(s^2+s+1)^3}{(s(s+1))^2} \quad \text{and} \quad j_{\mathrm{split},3}(t) = 12^3 \left(\frac{4t+4}{t^2-4} \right)^3.$$

This allows us to explicitly compute the fiber product $X_{\mathrm{split}}(3) \times_{X(1)} X(2)$ by equating $j_2(s) = j_{\mathrm{split},3}(t)$, and we let X to be the desingularization of this fiber product. We compute that X has genus 1 and 6 cusps, all contained in $X(\mathbb{Q})$. We turn X into an elliptic curve over $\mathbb{Q}$ by taking one of the cusps as the origin. Now X is isomorphic over $\mathbb{Q}$ to the elliptic curve determined by $y^2 = x^3 - 15x + 22$. This curve has rank 0 and torsion group of order 6. This shows that $X(\mathbb{Q})$ is exactly the set of cusps, which proves the proposition. ∎

Corollary 3.3 *Let $E/\mathbb{Q}$ be an elliptic curve with full rational 2-torsion. If ρ_3^E is irreducible, then ρ_3^E is strongly irreducible.*

Proof This follows immediately by combining Lemmas 3.1 and 3.2. ∎

We still need a nice criterion for deciding if ρ_3^E is irreducible.

Lemma 3.4 *Let $\mathcal{E}/\mathbb{F}_p$ be an elliptic curve over $\mathbb{F}_p$ and let a be the trace of Frobenius of this curve. Then $\mathcal{E}$ has a 3-isogeny over $\mathbb{F}_p$ if and only if $a \equiv \pm(p+1) \pmod 3$.*

Proof Note that $\mathcal{E}$ has a 3-isogeny over $\mathbb{F}_p$, if and only if either $\mathcal{E}$ or its quadratic twist $\mathcal{E}'$ has a 3-torsion point over $\mathbb{F}_p$, *i.e.*, $3 | \#\mathcal{E}(\mathbb{F}_p) = p+1-a$ or $3 | \#\mathcal{E}'(\mathbb{F}_p) = p+1+a$. This proves the lemma. ∎

This brings us to the criterion we need for checking strong irreducibility.

Proposition 3.5 *Let $E/\mathbb{Q}$ be an elliptic curve with full rational 2-torsion and $p \equiv 1 \pmod 3$ a prime of good reduction for E. If $3 | a_p(E)$, then ρ_3^E is strongly irreducible.*

Proof Corollary 3.3 tells us that irreducibility and strong irreducibility in our situation are equivalent. If ρ_3^E is reducible, then $E/\mathbb{Q}$ has a rational 3-isogeny, which implies $\overline{E}/\mathbb{F}_p$ has a 3-isogeny over $\mathbb{F}_p$ for all primes of good reduction p. By Lemma 3.4 this implies that if $p \equiv 1 \pmod 3$, then we have $a_p(E) \neq 0 \pmod 3$, which is the desired result. ∎

4 Twisted Fermat Equations

Let a, b, c be pairwise coprime nonzero integers and let $n > 1$ be an odd integer (the case n even is trivial, due to our sign choices). We are interested in solving the Diophantine equation

$$ax^n + by^n + cz^n = 0. \tag{4.1}$$

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

For $n > 3$, we know that this equation defines a curve C_n of genus greater than one, so by Faltings' theorem we get that $C_n(\mathbb{Q})$ is finite for any such n. In fact, in all the cases we will consider in this paper, we prove that $C_n(\mathbb{Q})$ is empty for all $n > 3$, except for one trivial solution when $n = 7$ in one of our examples. For $n > 3$ a prime, we will use the modular methods following [5, 6]. For $n = 3$, however, $C_3(\mathbb{Q}) \neq \varnothing$ and the Jacobian of the curve C_3, given by the equation

$$Y^2 = X^3 - 2^4 3^3 (abc)^2, \tag{4.2}$$

is an elliptic curve of positive rank in all the cases we are considering. The only remaining case is when $n = 9$, and we note that for our examples, C_9 has local points everywhere. We use our level lowering results modulo prime powers to show that $C_9(\mathbb{Q})$ is also empty.

From a Diophantine point of view, the main result is the following theorem.

Theorem 4.1 *Assume* (a, b, c) *is one of* $(5^2, 2^4, 23^4)$, $(5^8, 2^4, 37)$, $(5^7, 2^4, 59^7)$, $(7, 2^4, 47^7)$, *and* $(11, 2^4, 5^2 \cdot 17^2)$. *Then for* $n \in \mathbb{Z}_{\geq 2}$ *with* $n \neq 3$ *the twisted Fermat equation* (4.1) *has no solutions* x, y, z *in integers with* $xyz \neq 0$.

Remark 4.2 Since we are choosing a, b, and c all positive, proving that there are no solutions when n is even is trivial. Of course, by different choice of signs, one has to work a little bit harder, and we leave those cases to the interested reader.

In a sense, we have a complete description of the solutions for all the exponents $n > 1$, since we can find explicit generators for the Mordell-Weil group of the elliptic curve associated with C_3 over $\mathbb{Q}$.

4.1 The Modular Method

We review how to use elliptic curves, modular forms, and Galois representations to approach Diophantine equations of the form (4.1), mainly following [5]. We remark that we deviate from *loc. cit.* by allowing n to be a prime power instead of just a prime. Fix nonzero coprime integers a, b, c. Assume there is a solution in integers (x, y, z, n) to (4.1), with $xyz \neq 0$ and $n \geq 3$ odd. Without loss of generality we assume that by^n is even and that $ax^n \equiv -1 \pmod 4$. We also assume that ax^n, by^n, and cz^n are pairwise coprime. Consider the Frey elliptic curve

$$Y^2 = X(X - ax^n)(X + by^n).$$

This model is minimal at all odd primes. Furthermore, if $b \equiv 0 \pmod{16}$, then we can find a global minimal model over $\mathbb{Z}$

$$E_{n,(x,y)} : Y^2 + XY = X^3 + \frac{by^n - ax^n - 1}{4} X^2 - \frac{abx^n y^n}{16} X.$$

We often simply write E_n, or even E, when the indices are understood from the context. We assume that the condition on b is satisfied, since these are the only cases that

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

we will consider (for the general situation, the reader can refer to [5]). The minimal discriminant and the conductor of E_n are given by

$$\Delta(E_n) = \frac{(abcx^n y^n z^n)^2}{2^8}, \quad N(E_n) = \prod_{p|\Delta(E_n)} p.$$

Consider the Galois representation $\rho_n^{E_n}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Assume $n = l^r$ is a prime power with l an odd prime and r a positive integer, and that $\rho_l^{E_n}$ is strongly irreducible. By Ribet's level lowering [8, 9] and the work of Wiles and Taylor–Wiles [14, 15], we know that $\rho_l^{E_n}$ arises from a newform class f of (weight 2 and) level

$$N_0 = \prod_{\substack{p|abc \\ p>2}} p.$$

This means that there exists a prime ideal $\lambda \subset \mathcal{O}_f$ lying above l such that

$$\rho_l^{E_n} \simeq \rho_\lambda^f. \tag{4.3}$$

Remark 4.3 Note that since we are assuming that a, b, and c are pairwise coprime to each other, if $p^n \nmid abc$ with p prime, then for showing that (4.1) has no nontrivial solutions, we can assume without loss of generality that ax^n, by^n, and cz^n are pairwise coprime. This is the case for all of our examples when $n > 7$. In general, if for some prime p, we have that p divides ax^n, by^n, and cz^n, then it is possible that E_n has additive reduction at p, however for odd primes p, a quadratic twist of E_n will have a semistable reduction at p. We will replace E_n by its appropriate quadratic twist (if necessary) for the rest of this paper. For all our practical calculations we do not need to consider this situation separately as we will briefly explain now. First of all, we only consider the traces of Frobenius of E_n up to sign. The only computational difference left is that we might end up at a level N_0' dividing N_0; however, if we use the level N_0, all arguments still go through. This is because (4.3) not only holds for some newform class f of level N_0', but also still holds for some newform class f of level N_0. (The situation at the prime 2 is a bit more subtle; however, we do not have to deal with it when $n \geq 5$ in our examples.) Note that if we use the smaller level, the argument can be easier. For instance, in the example

$$5^7 x^n + 2^4 y^n + 59^7 z^n = 0,$$

when $n = 7$, we only need to consider newform classes of level 1 (of which there are none). This gives us a considerably easier contradiction. However, for sake of uniformity, we actually deal with newform classes of level 295 to show that this equation has no nontrivial solutions.

For every equation in Theorem 4.1, the level N_0 we need to consider is given in Table 4.1. By comparing traces of Frobenius, we obtain the congruences (i) and (ii) with $r = 1$. If (f, λ) is the unique pair of newform class f of level N_0 and prime $\lambda \subset \mathcal{O}_f$ lying above l that satisfies (4.3), λ is unramified, and for all primes $p|N_0$ we have $l \nmid v_p(\Delta(E_n))$, then we can apply Theorem 2.3 to $\rho_n^{E_n}$. In this case we get that $\rho_n^{E_n} \simeq \rho_{\lambda^r}^f$ and in particular that the congruences (i) and (ii) hold.

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

4.1.1 $l \geq 5$

Let $l \geq 5$ be a prime number. Note that by the arguments of [12, Proposition 6] we have that $\rho_l^{E_l}$ is irreducible, since E is semistable and has full rational 2-torsion (by our earlier remarks, this tells us that $\rho_l^{E_l}$ is strongly irreducible). In order to prove that there are no solutions to (4.1) for $n = l$, it suffices to find a contradiction (using congruences) to (4.3) for all pairs (f, λ) of newform classes f of level N_0 and primes $\lambda \subset \mathcal{O}_f$ lying above l.

Let f be a newform class of level N_0 such that (4.3) holds for some λ. For any prime p, define

$$\mathcal{A}_p = \begin{cases} \{a \in \mathbb{Z} : a \equiv p+1 \pmod 4 \text{ and } |a| \leq 2\sqrt{p}\} & \text{if } p \text{ is odd,} \\ \{-1, 1\} & \text{if } p = 2. \end{cases}$$

We claim that for all primes p where E has good reduction, we have $a_p(E) \in \mathcal{A}_p$. This is because E has full rational 2-torsion, and for an odd prime p of good reduction, $E[2]$ injects into the reduction of E modulo p. If E has good reduction at $p = 2$, then one checks that the reduction of E modulo p still has a rational 2-torsion point. Together with the Weil bound, the claim follows. Next, define for all primes p the set

$$\mathcal{T}_p = A_p \cup \{\pm(p+1)\}.$$

The congruences (i),(ii) with $r = 1$ now give us that for a prime $p \nmid N_0$ we have

$$l \,|\, L_{f,p} := p \prod_{a \in \mathcal{T}_p} \mathrm{Norm}(a - a_p(f)).$$

(If the degree of f is equal to 1, then the prime p before the product is not necessary, but in all our examples this does not lead to any new information.) It is of course possible that $L_{f,p} = 0$, in which case $l | L_{f,p}$ does not give any information. However, all our examples are chosen such that either f is not rational or it is rational and the elliptic curve of conductor N_0 associated with it by the Eichler–Shimura relation is not isogenous to an elliptic curve with full rational 2-torsion. In what follows, assume that f satisfies these conditions. This implies that for infinitely many (in fact, a positive proportion of) primes p we have $a_p(f) \notin \mathcal{A}_p$ (and hence $a_p(f) \notin \mathcal{T}_p$, since by the Weil bounds $a_p(f) \neq \pm(p+1)$). It is easy to get an upper bound in terms of N_0 (or a, b, c) for the smallest prime $p \nmid N_0$ for which $a_p(f) \notin \mathcal{A}_p$. In practice, for several primes $p_{\max}$, we compute

$$\gcd\left\{L_{f,p} : \text{ primes } p \leq p_{\max} \text{ with } p \nmid N_0\right\}$$

and the set of odd primes dividing this quantity, denoted $\mathcal{L}_{f,p_{\max}}$. We do this until we find a prime $p_{\max}$ for which $\mathcal{L}_{f,p_{\max}}$ is not empty and appears to be the same as $\mathcal{L}_{f,p'_{\max}}$ for any prime $p'_{\max} \geq p_{\max}$. This yields the information that for all primes $l > 3$ such that $l \notin \mathcal{L}_{f,p_{\max}}$ we have a contradiction to (4.3) for all primes $\lambda \subset \mathcal{O}_f$ lying above l.

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

For the given level N_0, let us finally define for a prime $p_{\max}$ the set

$$\mathcal{L}_{p_{\max}} = \bigcup_f \mathcal{L}_{f,p_{\max}},$$

where the union is over all newform classes f of level N_0. By taking $p_{\max}$ to be the maximum of the $p_{\max}$'s for the newform classes f, we arrive at a finite set of odd primes $\mathcal{L}_{p_{\max}}$ that contains 3 and, in practice, just a few other odd primes. For every equation in Theorem 4.1, a value of $p_{\max}$ together with $\mathcal{L}_{p_{\max}} - \{3\}$ is given in Table 4.1. The significance for the original Diophantine problem is that for every odd prime $l \notin \mathcal{L}_{p_{\max}}$ we have that (4.1) has no integer solutions with $xyz \neq 0$.

In our examples, for the finitely many primes $l \geq 5$ contained in $\mathcal{L}_{p_{\max}}$, we show that $C_l(\mathbb{Q}) = \varnothing$ (except for the one trivial exception) either by finding a prime p for which $C_n(\mathbb{Q}_p) = \varnothing$ or, if no such prime p exists, by using Kraus' method of reduction, see [7] or [5, Section 1.2.], which we briefly describe now.

Fix a prime power exponent $n = l^r$ (in *loc. cit.* n is assumed to be a prime). The possibilities for $a_p(E_n)$ (and $\mathrm{trace}(\rho_l^{E_n}(\mathrm{Frob}_p))$) with $p \equiv 1 \pmod{l}$ can sometimes be shown to be strictly smaller than $\mathcal{A}_p$, (and $\mathcal{T}_p$ respectively) by using the additional information that (4.1) has to be satisfied modulo p. Let $p \nmid lN_0$ be a prime. For an element $q \in \mathbb{Q}$ whose denominator is not divisible by p, we denote by $\overline{q}$ the reduction of q modulo p in $\mathbb{F}_p$. If (4.1) has an integer solution (x, y, z) with $p|xyz$ other than $(0, 0, 0)$, then necessarily one of

$$\overline{a/b}, \overline{b/c}, \text{ or } \overline{c/a} \text{ is in } \mathbb{F}_p^{*n}. \tag{4.4}$$

In this case we get from $\rho_l^{E_{n,(x,y)}} \simeq \rho_l^f$ that $a_p(f) \equiv \pm(p+1) \pmod{\lambda}$. If the (hypothetical) integer solution (x, y, z) to (4.1) satisfies $p \nmid xyz$, then $(\overline{x}, \overline{y})$ belongs to

$$S_{n,p} = \{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_p^* : \overline{a}\alpha^n + \overline{b}\beta^n + \overline{c}\gamma^n = 0 \text{ for some } \gamma \in \mathbb{F}_p^*\}.$$

For any $P = (\alpha, \beta) \in S_{n,p}$, define an elliptic curve over $\mathbb{F}_p$ by

$$\mathcal{E}_{n,p,P} : y^2 = x(x - \overline{a}\alpha^n)(x + \overline{b}\beta^n).$$

Then $a_p(E_{n,(x,y)})$ belongs to

$$\mathcal{A}_{n,p} = \{a_p(\mathcal{E}_{n,p,P}) : P \in S_{n,p}\}.$$

Also consider the set (of possibilities for $\mathrm{trace}(\rho_l^{E_n}(\mathrm{Frob}_p))$)

$$\mathcal{T}_{n,p} = \begin{cases} \mathcal{A}_{n,p} \cup \{\pm(p+1)\} & \text{if (4.4) holds,} \\ \mathcal{A}_{n,p} & \text{otherwise.} \end{cases}$$

Hence, in order to prove that for a (hypothetical) solution (x, y, z, n) to (4.1) and a certain newform class f of level N_0 we cannot have $\rho_l^{E_{n,(x,y)}} \simeq \rho_\lambda^f$ for any prime $\lambda \subset \mathcal{O}_f$ lying above l, it suffices to find a prime $p \nmid N_0 l$ such that

$$l \nmid \prod_{a \in \mathcal{T}_{n,p}} \mathrm{Norm}(a - a_p(f)).$$

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

If for all newform classes f of level N_0 we can find such a prime p, then we conclude that (4.1) has no integer solutions with $xyz \neq 0$. In practice, since we already computed $\mathcal{L}_{f,p_{\max}}$ for some "large" prime $p_{\max}$, it only remains to find such a prime p for the newform classes f of level N_0 for which $l \in \mathcal{L}_{f,p_{\max}}$.

Remark 4.4 From a computational point of view, it is worthwhile to consider $\mathcal{E}_{n,p,P}$ only up to quadratic twist in order to determine $\mathcal{A}_{n,p}$ (and hence $\mathcal{T}_{n,p}$). To be specific, let

$$S'_{n,p} = \{\alpha \in \mathbb{F}_p^* : \overline{a/c}\alpha^n + \overline{b/c} \in \mathbb{F}_p^{*n}\}.$$

Then we get

$$\mathcal{A}_{n,p} = \{\pm a_p(\mathcal{E}_{n,p,(\alpha,1)}) : \alpha \in S'_{k,p}\}.$$

For every equation in Theorem 4.1, an entry (l, p) under "local (l, p)" of Table 4.1 indicates that $C_l(\mathbb{Q}_p) = \varnothing$. Furthermore, for every prime $l \geq 5$ and newform class f of level N_0 for which $l \in \mathcal{L}_{f,p_{\max}}$ (which implies $l \in \mathcal{L}_{p_{\max}}$) and C_l is locally solvable everywhere, there is an entry (l, p) in Table 4.1 under "Kraus (l, p)" indicating that $l \nmid \prod_{a\in\mathcal{T}_{l,p}} \mathrm{Norm}(a - a_p(f))$. This completes the data that proves Theorem 4.1 for primes $l \geq 5$.

(a, b, c)	level	$p_{\max}$	$\mathcal{L}_{p_{\max}} - \{3\}$	local (l, p)	Kraus (l, p)
$(5^2, 2^4, 23^4)$	115	3	$\{5\}$	$(5, 11)$	–
$(5^8, 2^4, 37)$	185	3	$\{5, 19\}$	$(19, 19)$	$(5, 31)$
$(5^7, 2^4, 59^7)$	295	3	$\{5, 7\}$	$(5, 5)$	$(7, 43)$
$(7, 2^4, 47^7)$	329	23	$\{5\}$	–	$(5, 11)$ and $(5, 41)$
$(11, 2^4, 5^2 \cdot 17^2)$	935	71	$\{5, 7\}$	$(5, 5)$	$(7, 29)$

Table 4.1: Data for primes $l \geq 5$.

4.1.2 $n = 9$

To prove that $C_9(\mathbb{Q}) = \varnothing$ for our curves, we first note that C_9 has points everywhere locally; this is a straightforward computation. We can also quickly find a rational point on C_3 and find that the corresponding elliptic curve has positive rank over $\mathbb{Q}$; see Table 4.2. Next, we start applying a mod-3 modular approach. Before we can apply level lowering, we need to show that $\rho_3^{E_9}$ is irreducible (which implies that it is absolutely irreducible). Later on, we shall need the stronger result that $\rho_3^{E_9}$ is strongly irreducible. Using Proposition 3.5 we obtain an explicit criterion for checking this.

Proposition 4.5 *Suppose p is a prime such that*

- $p \nmid abc$;
- $p \equiv 1 \pmod 9$;
- *condition* (4.4) *does* not *hold;*
- *for all $P \in S_{9,p}$ we have $3|a_p(\mathcal{E}_{9,p,P})$.*

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

Then $\rho_3^{E_9}$ is strongly irreducible.

Proof Since we are assuming that $p \nmid abc$ and that condition (4.4) does not hold, we get that E_9 must have good reduction at p. Now for some $P \in S_{9,p}$ we have $a_p(E_9) = a_p(\mathcal{E}_{9,p,P})$. So the fourth assumption gives us that $3|a_p(E_9)$. Together with the assumption $p \equiv 1 \pmod 9$, the required result follows by Proposition 3.5. ■

Notice that, as in Remark 4.4, by considering quadratic twists, the last condition in the proposition above can be replaced by: for all $\alpha \in S'_{9,p}$, we have $3|a_p(\mathcal{E}_{9,p,(\alpha,1)})$. In all our examples, we find a prime $p = p_{\text{irr}}$ satisfying all the conditions in the proposition above, the (smallest) value is recorded in Table 4.2.

Although we would like to apply Theorem 2.3 with $r = 2$ and $l = 3$, for most of the levels N_0 we are considering there actually exist distinct pairs $(f_1, \lambda_1), (f_2, \lambda_2)$ of newform classes f_1, f_2 of level N_0 and prime ideals $\lambda_i \subset \mathcal{O}_{f_i}$ $(i = 1, 2)$ lying above 3 for which $\rho_{f_1}^{\lambda_1} \simeq \rho_{f_2}^{\lambda_2}$ holds. So we start with applying "ordinary" level lowering mod-3. For every newform class f of level N_0 with $3 \in \mathcal{L}_{f,p_{\max}}$ we compute for various primes $p \nmid abc$ with $p \equiv 1 \pmod 3$ the set $\mathcal{T}_{9,p}$ and check if

$$3 \nmid \prod_{a \in \mathcal{T}_{9,p}} \text{Norm}(a - a_p(f)). \tag{4.5}$$

Denote by $\mathcal{N}_{p_0}$ the set of newform classes f of level N_0 such that for all primes $p \leq p_0$, (4.5) does not hold. The prime p_0 we used, together with a description of $\mathcal{N}_{p_0}$, is given in Table 4.2. Now if $\rho_3^{E_9} \simeq \rho_\lambda^f$ for some newform class f of level N_0 and prime ideal $\lambda \subset \mathcal{O}_f$ lying above 3, then necessarily $f \in \mathcal{N}_{p_0}$. For all the cases we consider, taking into account that the image of the representation has to be contained in $\text{GL}_2(\mathbb{F}_3)$, we find that λ has to be of inertia degree 1. Furthermore, we find a p_0 such that $\mathcal{N}_{p_0}$ is small enough so that the uniqueness condition in Theorem 2.3 now holds. As for the ramification condition, in all our cases, except when $N_0 = 935$, we find that 3 is unramified in K_f for all $f \in \mathcal{N}_{p_0}$. For the case where $N_0 = 935$, we actually find that the pair (f, λ) we cannot deal with modulo 3 has λ ramified in K_f, and we deal with this case by studying the deformation ring directly. In all other cases, we apply Theorem 2.3 (with $r = 2$ and $l = 3$) to all newform classes in $\mathcal{N}_{p_0}$. This time, for all $f \in \mathcal{N}_{p_0}$, we simply try to find a prime $p \nmid 3N_0$ such that for all $a \in \mathcal{T}_p$ we have

$$9 \nmid \text{Norm}(a - a_p(f)) \quad \text{and} \quad \mathbb{Q}(a_p(f)) = K_f.$$

In all cases we readily find such a prime p; for the value, see Table 4.2. This means that we also obtain a contradiction from $\rho_9^{E_9} \simeq \rho_{\lambda^2}^f$ for all $f \in \mathcal{N}_{p_0}$ and all relevant λ. It follows that $C_9(\mathbb{Q}) = \varnothing$.

Remark 4.6 In other cases, using $\mathcal{T}_p$ might not give enough information. Using $\mathcal{T}_{9,p}$ instead might lead to the desired conclusion. Furthermore, computing $a_p(f) \pmod \lambda$ may yield more information than $\text{Norm}(a - a_p(f)) \pmod l$. For example, if $(a, b, c) = (7, 2^4, 47^7)$, computing $\text{Norm}(a - a_p(f)) \pmod 3$ did not give us enough information to rule out the newform classes of level 329 with degrees 5 and

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

level	$\mathbb{Q}$-rank of C_3	p_{irr}	p_0	$\mathcal{N}_{p_0}$ description	p
115	2	73	–	$d = 1$	2
185	1	73	73	$d = 1^*$	2
295	2	37	37	$d = 6$	13
329	2	109	13	$d = 5, d = 6$	5,5
935	2	37	37	$d = 11^*$	–

Table 4.2: Data for $n = 3$ and $n = 9$; d denotes the degree of the newform class. In case of a $*$, the degree alone does not determine the class uniquely, in which case we impose the extra condition $\text{trace}(a_2(f)) = 0$, which does determine the class uniquely.

6. However, the newform class f of degree 6 can be ruled out using $a_p(f) \pmod{\lambda}$. Specifically, there is a unique prime λ above 3 of inertia degree 1 in K_f. For any other prime λ' above 3, the image of the Galois representation $\rho^f_{\lambda'}$ is not contained in $\mathrm{GL}_2(\mathbb{F}_3)$, hence not isomorphic to $\rho_3^{E_9}$. To rule out the prime λ in this case, we just note that $f \pmod{\lambda}$ is an Eisenstein series, which means ρ^f_λ is reducible, hence not isomorphic to $\rho_3^{E_9}$, since we proved this is irreducible.

In fact, using these observations, in all our cases we find that there is exactly one pair of (f, λ) for which we are unable to obtain a contradiction using just level lowering modulo 3. In Section 5 we will prove that level lowering modulo 3 is not sufficient for this pair.

4.1.3 Level 935

We now consider the example

$$11x^9 + 2^4y^9 + 5^2 \cdot 17^2z^9 = 0.$$

Using the data in Table 4.2, we conclude that if there is a nontrivial solution to this equation, then we have $\rho_3^{E_9} \not\simeq \rho_\lambda^{f_{11}}$, where f_{11} is the newform class of level 935 with degree 11 and $\text{trace}(a_2(f_{11})) = 0$, and $\lambda \subset \mathcal{O}_{f_{11}}$ is a prime lying above 3 of inertia degree 1. There are exactly two primes $\lambda_1, \lambda_2 \subset \mathcal{O}_{f_{11}}$ lying above 3 of inertia degree 1. One is unramified, say λ_1, but the other, say λ_2, is ramified. As for the representations $\rho^{f_{11}}_{\lambda_i}$ for $i = 1, 2$, we quickly find that they are not isomorphic.

The case $\rho_3^{E_9} \simeq \rho^{f_{11}}_{\lambda_1}$ actually leads to a contradiction fairly easily by computing $\mathcal{T}_{9,31} = \{\pm 8, \pm 32\}$ and $a_{31}(f_{11}) \equiv 0 \pmod{\lambda_1}$.

The situation for (f_{11}, λ_2) is a bit more delicate, specially since we can not apply our level lowering theorem in this situation. However we can still rule this case out by using the deformation ring directly. Assume that $\rho_3^{E_9} \simeq \rho^{f_{11}}_{\lambda_2}$. Then $\rho_9^{E_9}$ is a minimal deformation of $\rho^{f_{11}}_{\lambda_2}$. Therefore, this representation should correspond to a unique map $\mathbb{R}^{\text{univ}} \to \mathbb{Z}/9\mathbb{Z}$. However, we can explicitly compute $\mathbb{R}^{\text{univ}} = \mathbb{T}$, as we did in Remark 2.9. Since (f_{11}, λ_2) is not congruent to any other newform class of level 935, we get that $\mathbb{T} = \left(\mathcal{O}_{f_{11}}\right)_{\lambda_2}$. Using SAGE or MAGMA we get that $\mathbb{Z}[a_3(f_{11})] \subset \mathcal{O}_{f_{11}}$ with an index coprime to 3. Therefore,

$$\mathcal{O}_{f_{11}} \otimes \mathbb{Z}_3 = \mathbb{Z}_3[T]/\langle P(T)\rangle,$$

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

where

$$P(T) = T^{11} - T^{10} - 25T^9 + 26T^8 + 222T^7 - 225T^6 - 827T^5 + 705T^4 + 1212T^3 - 449T^2 - 770T - 168$$

is the minimal polynomial for $a_3(f_{11})$. Factoring $P(T)$ over $\mathbb{Z}_3$, we can conclude that

$$\mathbb{T} = \left(\mathcal{O}_{f_{11}}\right)_{\lambda_2} = \mathbb{Z}_3[T]/\langle T^2 - aT + b\rangle$$

where $a \equiv 4 \pmod 9$ and $b \equiv 7 \pmod 9$. Looking at the above equation modulo 9, we get $T^2 - aT + b \equiv (x-2)^2 + 3 \pmod 9$, which implies that there are no maps $\mathbb{T} \to \mathbb{Z}/9\mathbb{Z}$. This gives us a contradiction to our assumption that $\rho_9^{E_9}$ is a minimal deformation of $\rho_{\lambda_2}^{f_{11}}$, which rules this modular form out as well and proves our result.

5 Necessity of Level Lowering Modulo 9

One can ask if we really needed level lowering modulo 9 for solving (4.1). A priori it could be possible that by using level lowering modulo 3 we can already obtain the desired contradictions. However, we will show that for our choice of Frey curve and triples (a, b, c), level lowering modulo 3 does not yield enough information.

Remark 5.1 We note that there are Frey curves attached to the Diophantine equations

$$ax^n + by^n + cz^3 = 0, \quad ax^3 + by^3 + cz^n = 0,$$

and we can specialize these curves to the case $n = 9$. The Frey curve attached to the first equation has a rational 3-isogeny by construction, so it is not suitable for level lowering. As for the Frey curves attached to the second equation, along similar lines as in Section 3, one can show that $E[3]$ is strongly irreducible. However, we end up having to deal with modular forms of higher level, for example when $(a, b, c) = (11, 2^4, 5^2 \cdot 17^2)$, we have to deal with modular forms of level (at least) 92565, which is computationally very difficult.

We also note that other possible non-modular approaches to proving $C_9(\mathbb{Q}) = \varnothing$ include descent methods and Mordell–Weil sieving. This is a promising approach, almost completely orthogonal to the modular method presented here, and can be an interesting topic for further investigation.

Let $\overline{\mathcal{T}_{n,p}} \subset \mathbb{F}_3$ be the image of $\mathcal{T}_{n,p}$ under the reduction map modulo 3. In this section we will show that for our examples, the unique pair of newform class f of level N_0 and prime $\lambda \subset \mathcal{O}_f$ lying above 3 mentioned at the end of Remark 4.6 satisfies

$$a_p(f) \mod \lambda \in \overline{\mathcal{T}_{9,p}}$$

for all primes $p \nmid 3N_0$. This means that level lowering modulo 9 (along with the argument in Section 4.1.3) is necessary to prove Theorem 4.1.

We will start by showing that $\overline{\mathcal{T}_{3,p}} \neq \mathbb{F}_3$ infinitely often, by showing $0 \notin \overline{\mathcal{T}_{3,p}}$ for infinitely many $p \equiv 1 \pmod 3$.

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

Lemma 5.2 *Let $j\colon C_n \to X(2) \to X(1)$ be the j-invariant of the Frey elliptic curve corresponding to a point on C_n, let $p \equiv 1 \pmod{n}$ be a prime with $p \nmid N_0 n$, and let $\pi\colon X_0(3) \to X(1)$ be the natural forgetful map between the modular curves. Then*

(i) *$0 \notin \overline{\mathcal{T}_{n,p}}$ if and only if $j(C_n(\mathbb{F}_p)) \subset \pi(X_0(3)(\mathbb{F}_p))$ if and only if*

$$\left(C_n \times_{X(1)} X_0(3)\right)(\mathbb{F}_p) \to C_n(\mathbb{F}_p)$$

is surjective;

(ii) *$\pm 1 \in \overline{\mathcal{T}_{n,p}}$, if and only if there is a $z \in C_n(\mathbb{F}_p)$ such that $j(z) \in \pi(X_0(3)(\mathbb{F}_p))$ if and only if $\left(C_n \times_{X(1)} X_0(3)\right)(\mathbb{F}_p)$ is not empty.*

Proof If $0 \notin \overline{\mathcal{T}_{n,p}}$, then by Lemma 3.4 we get that for all $z \in j(C_n(\mathbb{F}_p))$ such that $z \neq \infty$ we have that the corresponding elliptic curve $\mathcal{E}_n/\mathbb{F}_p$ has a 3-isogeny, *i.e.*, $z \in \pi(X_0(3)(\mathbb{F}_p))$. We also know that $\infty \in \pi(X_0(3)(\mathbb{F}_p))$, therefore we get $j(C_n(\mathbb{F}_p)) \subset \pi(X_0(3)(\mathbb{F}_p))$. Now assume that $j(C_n(\mathbb{F}_p)) \subset \pi(X_0(3)(\mathbb{F}_p))$. Let $z \in j(C_n(\mathbb{F}_p))$. Notice that if $z = \infty$, then the trace of Frobenius of the corresponding generalized elliptic curve is $\pm(p+1) \not\equiv 0 \pmod{3}$. If $z \neq \infty$, then by our assumption z corresponds to an elliptic curve $\mathcal{E}_n/\mathbb{F}_p$ with a rational three isogeny, which by Lemma 3.4 will have trace of Frobenius equivalent to ± 1 modulo 3. In either case we get $0 \notin \overline{\mathcal{T}_{n,p}}$. This proves the first equivalence. By the definition of fiber products we see that $j(C_n(\mathbb{F}_p)) \subset \pi(X_0(3)(\mathbb{F}_p))$ if and only if $\left(C_n \times_{X(1)} X_0(3)\right)(\mathbb{F}_p) \to C_n(\mathbb{F}_p)$ is surjective, which finishes the first part of the lemma.

The second part of the lemma is proved in a similar fashion. ∎

Therefore, to find primes p such that $0 \notin \overline{\mathcal{T}_{3,p}}$, we are reduced to finding p such that $(C_3 \times_{X(1)} X_0(3))(\mathbb{F}_p) \to C_3(\mathbb{F}_p)$ is not surjective. For brevity, we will drop the $X(1)$ from the fiber product. Let $\widetilde{C_3 \times X_0(3)}$ be the desingularization of the fiber product. The following lemma describes the map $\widetilde{C_3 \times X_0(3)} \to C_3$.

Lemma 5.3 *The curve $C_3 \times X_0(3)$ is a genus one curve. Furthermore, the natural map $\widetilde{C_3 \times X_0(3)} \to C_3$ induces the multiplication by 2 map on their Jacobians. In particular, the Jacobian of C_3 is isomorphic to the Jacobian of $\widetilde{C_3 \times X_0(3)}$.*

Proof A quick calculation shows that for every point P of $X(1)$, the ramification indices of $X_0(3) \to X(1)$ above P all divide the ramification indices of $C_3 \to X(1)$ above P, which implies that

$$\widetilde{C_3 \times X_0(3)} \longrightarrow C_3$$

is unramified. Therefore, by Riemann–Hurwitz's theorem we get that $\widetilde{C_3 \times X_0(3)} \to X(1)$ is a genus one curve.

To show that this map is the multiplication by 2 map on the Jacobians, note that this a geometric statement, and it suffices to prove it for a particular twist of C_3. Specifically, we show that $\widetilde{C \times X_0(3)} \to C$ over $\mathbb{Q}$ induces the multiplication by 2 map on the Jacobians, where $C : x^3 + y^3 + z^3 = 0$. The induced map on the Jacobians

$$\mathrm{Jac}(C) \longrightarrow \mathrm{Jac}\left(\widetilde{C \times X_0(3)}\right)$$

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

is an isogeny of degree 4, and is defined over $\mathbb{Q}$. Notice that $\mathrm{Jac}(C)$ is the elliptic curve given by $Y^2 = X^3 - 2^4 \cdot 3^3$. This elliptic curve has no rational 2 isogeny, therefore the only possibility is for the above map to be multiplication by 2, which is the desired result. ∎

The following proposition tells us that for most problems, $0 \notin \overline{\mathcal{T}_{3,p}}$ for infinitely many primes p.

Proposition 5.4 *Let J be the Jacobian of $C_3/\mathbb{Q}$ and let $p \equiv 1 \pmod 3$ be a prime. Assume that J has good reduction at p. Then $2|a_p(J)$ if and only if $0 \in \overline{\mathcal{T}_{3,p}}$. Specifically, if $4abc$ is not a perfect cube, then $0 \notin \overline{\mathcal{T}_{3,p}}$ infinitely often.*

Proof By Lemma 5.2, we need to show that $2|a_p(J)$ if and only if

$$\left(C_3 \times X_0(3)\right)(\mathbb{F}_p) \to C_3(\mathbb{F}_p)$$

is not surjective. Notice that we can replace $C_3 \times X_0(3)$ by its desingularization without loss of generality.

By Lemma 5.3, we know that $\widetilde{C_3 \times X_0(3)}$ is a genus one curve. Using the Weil bound we get that genus one curves always have an $\mathbb{F}_p$ point, and hence they are isomorphic to their Jacobians. Let $P \in (\widetilde{C_3 \times X_0(3)})(\mathbb{F}_p)$, and let Q be the image of this point in $C_3(\mathbb{F}_p)$. Using P and Q as the origins, we get an explicit isomorphism between $C_3 \simeq J \simeq \widetilde{C_3 \times X_0(3)}$. Using this identification, the map $\widetilde{C_3 \times X_0(3)} \to C_3$ is the multiplication by 2 map.

Now if we assume that $a_p(J)$ is odd, then $J(\mathbb{F}_p)$ is an Abelian group with an odd order, therefore the multiplication by 2 map is an isomorphism. In particular,

$$\left(\widetilde{C_3 \times X_0(3)}\right)(\mathbb{F}_p) \to C_3(\mathbb{F}_p)$$

is surjective. Similarly, if $a_p(J)$ is even, then $J(\mathbb{F}_p)$ is an Abelian group with even order, and therefore the multiplication by 2 map is not surjective on the $\mathbb{F}_p$ points.

Note that, when $4abc$ is not a perfect cube, the Jacobian J, given by (4.2), has no nontrivial rational 2-torsion point. In this situation, $a_p(J)$ is odd infinitely often, and we get that for infinitely many p's, $0 \notin \overline{\mathcal{T}_{3,p}}$. This completes the proof of the proposition. ∎

In all our cases, it is easy to find an integer solution (x, y, z) to (4.1) with $n = 3$ such that $\rho_3^{E_{3,(x,y)}} \simeq \rho_\lambda^f$. This shows that $a_p(f) \mod \lambda \in \overline{\mathcal{T}_{3,p}}$ for all primes $p \nmid 3N_0$. However, since

$$\overline{\mathcal{T}_{9,p}} \subset \overline{\mathcal{T}_{3,p}},$$

a priori it is possible that Kraus' argument can succeed for some prime p beyond our search space. This is in fact not the case, and we show that for p large enough, this containment is in fact equality, and hence we cannot get a contradiction (it is easy to see that for $p \equiv 2 \pmod 3$ we have $\overline{\mathcal{T}_{9,p}} = \overline{\mathcal{T}_{3,p}} = \mathbb{F}_3$).

Proposition 5.5 (i) *If $p > 216^2$ is a prime congruent to $1 \pmod 3$, then $\pm 1 \in \overline{\mathcal{T}_{3,p}}$ if and only if $\pm 1 \in \overline{\mathcal{T}_{9,p}}$.*

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

(ii) *If* $p > 106^2$ *is a prime congruent to* 1 (mod 3), *then* $0 \in \overline{\mathcal{T}_{3,p}}$, *if and only if* $0 \in \overline{\mathcal{T}_{9,p}}$.

Proof To prove the first part of the claim, by Lemma 5.2, we need to show $C_9 \times X_0(3)$ has an $\mathbb{F}_p$ rational point, however this follows from the Weil bound

$$\left|\left(\widetilde{C_9 \times X_0}(3)\right)(\mathbb{F}_p)\right| > p + 1 - 2g\sqrt{p},$$

where g is the genus of $C_9 \times X_0(3)$. To calculate this genus, note that $\widetilde{C_9 \times X_0}(3) \to C_9$ is unramified of degree 4, and we know that the genus of C_9 is $(9-1)(9-2)/2 = 28$. Therefore, using the Riemann–Hurwitz theorem we get that $g = 109$. Therefore,

$$\left|\left(\widetilde{C_9 \times X_0}(3)\right)(\mathbb{F}_p)\right| > p + 1 - 218\sqrt{p},$$

which means for $p > 218^2$, the curve $\widetilde{C_9 \times X_0}(3)$ will have an $\mathbb{F}_p$ point. This finishes the proof of the first part of the proposition.

To prove the second part, assume that $0 \in \overline{\mathcal{T}_{3,p}}$. Then, by Lemma 5.2 the map $(\widetilde{C_3 \times X_0}(3))(\mathbb{F}_p) \to C_3(\mathbb{F}_p)$ is not surjective. Assume that $(\widetilde{C_9 \times X_0}(3))(\mathbb{F}_p) \to C_9(\mathbb{F}_p)$ is surjective. We want to show that $p < 106^2$. Let $P \in C_9(\mathbb{F}_p)$. Then we can find a point $Q \in (\widetilde{C_9 \times X_0}(3))(\mathbb{F}_p)$ which maps to P. This implies that $\phi(P)$ is in the image of $(\widetilde{C_3 \times X_0}(3))(\mathbb{F}_p) \to C_3(\mathbb{F}_p)$. However, since this map is just multiplication by 2, and since it is not surjective, there are either 2 or 4 points that map to $\phi(P)$. This implies that there are either 2 or 4 points in $(\widetilde{C_9 \times X_0}(3))(\mathbb{F}_p)$ that map to P. Therefore,

$$\left|\left(\widetilde{C_9 \times X_0}(3)\right)(\mathbb{F}_p)\right| \geq 2|C_9(\mathbb{F}_p)|.$$

However, the Weil bound tell us that

$$|C_9(\mathbb{F}_p)| \geq p + 1 - 2 \cdot 28\sqrt{p},$$
$$\left|\left(\widetilde{C_9 \times X_0}(3)\right)(\mathbb{F}_p)\right| \leq p + 1 + 2 \cdot 109\sqrt{p}.$$

Using these estimates we get that $p < 106^2$, as desired. ∎

Remark 5.6 For the proof of Proposition 5.5, we used the most basic bounds for simplicity of the exposition. However, since the curves we are using are fairly special, much better bounds are known.

We can now readily find all primes p such that $\overline{\mathcal{T}_{9,p}} \neq \overline{\mathcal{T}_{3,p}}$. Table 5.1 collects this data: the column labeled p_0 is the set of primes such that $0 \in \overline{\mathcal{T}_{3,p}}$ but $0 \notin \overline{\mathcal{T}_{9,p}}$, and the column labeled p_1 is the set of primes such that $\pm 1 \notin \overline{\mathcal{T}_{9,p}}$. For all such primes, we can check that $a_p(f) \in \overline{\mathcal{T}_{9,p}}$, which proves that we cannot rule out f using mod 3 level lowering.

https://doi.org/10.4153/CJM-2011-059-8 Published online by Cambridge University Press

(a, b, c)	p_0	p_1
$(5^2, 2^4, 23^4)$	$\{73, 163\}$	$\varnothing$
$(5^8, 2^4, 37)$	$\{73, 307, 541\}$	$\{37\}$
$(5^7, 2^4, 59^7)$	$\{37, 73, 163, 181, 199, 541\}$	$\varnothing$
$(7, 2^4, 47^7)$	$\varnothing$	$\{109\}$
$(11, 2^4, 5^2 \cdot 17^2)$	$\{37, 73, 307, 541\}$	$\varnothing$

Table 5.1: Primes p where $\overline{\mathcal{T}_{3,p}} \neq \overline{\mathcal{T}_{9,p}}$.

References

[1] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem.* In: Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154.

[2] M. Darnell, C. Holden, B. Kane, J. Weinstein, and S. Yazdani, *MSRI modular forms summer workshop.* August 2006, http://www.math.ubc.ca/~syazdani/MSRI_archive

[3] F. Diamond, *On deformation rings and Hecke rings.* Ann. of Math. (2) **144**(1996), no. 1, 137–166. http://dx.doi.org/10.2307/2118586

[4] L. Dieulefait and X. Taixés i Ventosa, *Congruences between modular forms and lowering the level mod l^n.* J. Théor. Nombres Bordeaux **21**(2009), no. 1, 109–118.

[5] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes.* J. Reine Angew. Math. **548**(2002), 167–234. http://dx.doi.org/10.1515/crll.2002.058

[6] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée.* Canad. J. Math. **49**(1997), no. 6, 1139–1161. http://dx.doi.org/10.4153/CJM-1997-056-2

[7] ———, *Sur l'équation $a^3 + b^3 = c^p$.* Experiment. Math. **7**(1998), no. 1, 1–13.

[8] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms.* Invent. Math. **100**(1990), no. 2, 431–476. http://dx.doi.org/10.1007/BF01231195

[9] ———, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In: Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., 55, American Mathematical Society, Providence, RI, 1994, pp. 639–676.

[10] ———, *Images of semistable Galois representations. Olga Taussky-Todd: in memoriam.* Pacific J. Math. **1997**, Special Issue, 277–297. http://dx.doi.org/10.2140/pjm.1997.181.277

[11] K. Rubin, *Modularity of mod* 5 *representations.* In: Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 463–474.

[12] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**(1987), no. 1, 179–230. http://dx.doi.org/10.1215/S0012-7094-87-05413-5

[13] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan, 11, Kanô Memorial Lectures, 1, Princeton University Press, Princeton, NJ, 1994.

[14] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141**(1995), no. 3, 553–572. http://dx.doi.org/10.2307/2118560

[15] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141**(1995), no. 3, 443–551. http://dx.doi.org/10.2307/2118559

Department of Mathematics, The University of British Columbia, Vancouver, BC, V6T 1Z2
e-mail: dahmen@math.ubc.ca

Department of Mathematics and Statistics, McMaster University, West Hamilton, ON, L8S 4K1
e-mail: syazdani@math.mcmaster.ca