LMS J. Comput. Math. 15 (2012) 158–171 © 2012 Author
doi:10.1112/S146115701200006X

On the equations $a^2 - 2b^6 = c^p$ and $a^2 - 2 = c^p$

Imin Chen

Abstract

We study the equation $a^2 - 2b^6 = c^p$ and its specialization $a^2 - 2 = c^p$, where p is a prime, using the modular method. In particular, we use a $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ for which the solution $(a, b, c) = (\pm 1, \pm 1, -1)$ gives rise to a CM-form. This allows us to apply the modular method to resolve the equation $a^2 - 2b^6 = c^p$ for p in certain congruence classes. For the specialization $a^2 - 2 = c^p$, we use the multi-Frey technique of Siksek to obtain further refined results.

1. *Introduction*

The modular method has been successfully applied to a number of classes of ternary diophantine equations of the form $Aa^r + Bb^s = Cc^t$, where A, B, C are given non-zero integers, r, s, t are positive integers, and a, b, c are integer unknowns. Of interest sometimes are equations obtained by setting one of the variables a, b and c to 1.

The equation $a^2 - 2 = c^p$ is an example, but because the solution $(a, c) = (\pm 1, -1)$ is present for every p and the standard associated elliptic curves over $\mathbb{Q}$ from the modular method do not have complex multiplication, the modular method cannot be applied in full using these Frey curves [**4**].

By regarding this equation as a special case of $a^2 - 2b^6 = c^p$, we show that it is possible to associate a $\mathbb{Q}$-curve completely defined over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ to a hypothetical solution. The solution $(a, c) = (\pm 1, -1)$ now luckily corresponds to an elliptic curve with complex multiplication by the quadratic order of discriminant -24, and using $\mathbb{Q}$-curves [**8, 12**] the modular method can then be applied to obtain the results below.

Let p be a prime. We say that an integer solution $(a, b, c) \in \mathbb{Z}^3$ to $a^2 - 2b^6 = c^p$ is proper if $(a, b, c) = 1$ and trivial if $abc = 0$. Because $p > 1$, we note that an integer solution $(a, b, c) \in \mathbb{Z}^3$ is proper if and only if the integers a, b and c are pairwise coprime.

Theorem 1. *Let p be a prime such that $p \equiv 1, 7 \pmod{24}$ and $p \neq 7$. Then the equation $a^2 - 2b^6 = c^p$ does not have any non-trivial proper integer solutions except those with $c = \pm 1$.*

Although we can obtain partial results for this equation, it is in some sense a lucky coincidence that the solution $(\pm 1, \pm 1, -1)$ corresponds to a CM-form after using an appropriate Frey $\mathbb{Q}$-curve. The obstruction to obtaining complete results for the equation $a^2 - 2b^6 = c^p$ is due to the inapplicability of Mazur's method to studying rational points on certain non-split Cartan modular curves. This obstruction appears when applying the modular method to other equations, such as $a^2 + b^{2p} = c^5$ (see [**8**]), and is the same stumbling block that prevents an answer to Serre's question on the surjectivity of mod p representations attached to elliptic curves over $\mathbb{Q}$; see [**18, 24**].

The idea of considering the equation $a^2 - 2b^6 = c^p$ arose from work on the related equation $a^2 + b^6 = c^p$ (see [**1**]). As a consequence of Theorem 1, we obtain the following result on the specialization $a^2 - 2 = c^p$.

Received 4 October 2010; revised 15 September 2011.

2010 Mathematics Subject Classification 11D41 (primary), 14G05, 11G05, 11D61 (secondary).

This research was supported by NSERC.

COROLLARY 2. *Let p be a prime such that $p \equiv 1, 7 \pmod{24}$ and $p \neq 7$. Then the equation $a^2 - 2 = c^p$ does not have any integer solutions other than $(a, c) = (\pm 1, -1)$.*

For comparison, we list results on the above equation obtained with other methods. Using GP's built-in Thue equation solver, the following is shown in [**9**, Lemma 15.7.3].

LEMMA 3. *If $5 \leqslant p \leqslant 37$ is a prime, then the only integer solutions to $a^2 - 2 = c^p$ are $(a, c) = (\pm 1, -1)$.*

Using lower bounds for linear forms in logarithms due to Bugeaud, Mignotte and Siksek as well as Laurent, Mignotte and Nesterenko, it is noted in [**9**, p. 520] that the following holds.

THEOREM 4. *If $p > 8200$ is a prime, then the only integer solutions to $a^2 - 2 = c^p$ are $(a, c) = (\pm 1, -1)$.*

It is also noted in [**9**, p. 520] that the refinement $p \geqslant 1237$ can be derived from the additional information provided by [**9**, Lemma 15.7.2] and another careful application of linear forms in logarithms.

Using a multi-Frey technique [**3, 5**], it is possible to improve Corollary 2 to obtain the following result.

THEOREM 5. *Let p be a prime such that $p \equiv 1, 5, 7, 11 \pmod{24}$ and $p \neq 5, 7$. Then the equation $a^2 - 2 = c^p$ does not have any integer solutions other than $(a, c) = (\pm 1, -1)$.*

We thank S. Siksek for suggesting a lemma which allows us to apply the multi-Frey technique to $\mathbb{Q}$-curves.

The computations in this paper were performed with the computational algebra system Magma [**2**]. The programs, data and output files are posted at www.math.sfu.ca/~ichen/b3i-data. Throughout the text, specific references to the programs used are enclosed in boxes.

2. *Review of $\mathbb{Q}$-curves*

Let K be a number field and let C/K be a non-CM elliptic curve such that there is a non-zero isogeny $\mu_C(\sigma) : {}^\sigma C \to C$ defined over K for each $\sigma \in G_\mathbb{Q}$. Without loss of generality, we assume $\mu_C(\sigma) = 1$ for $\sigma \in G_K$. Such a curve C/K is called a $\mathbb{Q}$-curve defined over K. Let $\hat{\phi}_{C,p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$ be the representation of G_K on the Tate module $\hat{V}_p(C)$. One can attach a representation

$$\hat{\rho}_{C,\beta,\pi} : G_\mathbb{Q} \to \overline{\mathbb{Q}}_p^* \, \mathrm{GL}_2(\mathbb{Q}_p)$$

to C such that $\mathbb{P}\hat{\rho}_{C,\beta,\pi|_{G_K}} \cong \mathbb{P}\hat{\phi}_{C,p}$.

Let

$$\begin{aligned} c_C(\sigma, \tau) &= \mu_C(\sigma) {}^\sigma\mu_C(\tau) \mu_C(\sigma\tau)^{-1} \\ &\in (\mathrm{Hom}_K(C, C) \otimes_\mathbb{Z} \mathbb{Q})^* = \mathbb{Q}^* \end{aligned}$$

where $\mu_C^{-1} := (1/\deg \mu_C)\mu_C'$ and μ_C' is the dual of μ_C. Then $c_C(\sigma, \tau)$ determines a class in $H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ which depends only on the $\overline{\mathbb{Q}}$-isogeny class of C.

The class $c_C(\sigma, \tau)$ factors through $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$, and this class depends only on the K-isogeny class of C. Alternatively,

$$c_C(\sigma, \tau) = \alpha(\sigma) {}^\sigma\alpha(\tau) \alpha(\sigma\tau)^{-1}$$

arises from a class $\alpha \in H^1(G_\mathbb{Q}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$ through the map

$$H^1(G_\mathbb{Q}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*) \to H^2(G_\mathbb{Q}, \mathbb{Q}^*)$$

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

resulting from the short exact sequence

$$1 \to \mathbb{Q}^* \to \overline{\mathbb{Q}}^* \to \overline{\mathbb{Q}}^*/\mathbb{Q}^* \to 1.$$

Explicitly, $\alpha(\sigma)$ is defined by $\sigma^*(\omega_C) = \alpha(\sigma)\omega_C$, where ω_C is the invariant differential of C.

Tate showed that $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$ is trivial where the action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}^*$ is trivial. Thus, there is a continuous map $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ such that

$$c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$

as cocycles, and we call β a splitting map for c_C. We define

$$\hat{\rho}_{C,\beta,\pi}(\sigma)(1 \otimes x) = \beta(\sigma)^{-1} \otimes \mu_C(\sigma)(\sigma(x)).$$

The representation $\hat{\rho}_{C,\beta,\pi}$ depends on a choice of splitting map β. Let π be a prime above p of the field M_β generated by the values of β. The representation $\hat{\rho}_{C,\beta,\pi}$ is constructed in such a way that its image lies in $M^*_{\beta,\pi}\,\mathrm{GL}_2(\mathbb{Q}_p)$, and we choose to use the notation $\hat{\rho}_{C,\beta,p} = \hat{\rho}_{C,\beta,\pi}$ to indicate the choice of π in this explicit construction.

Given a splitting $c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$, Ribet attaches an abelian variety A_β defined over $\mathbb{Q}$ of GL_2-type having C as a simple factor over $\overline{\mathbb{Q}}$. Using results in [**21**], it is possible to identify $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ factoring over an extension of low degree such that $c_C = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$ *as classes* in $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$. It is then useful in practice to pick a suitable twist C_β/K_β of C such that $c_{C_\beta}(\sigma, \tau)$ is exactly the cocycle $c_\beta(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$. In this situation, the abelian variety A_β is constructed as a quotient over $\mathbb{Q}$ of $\mathrm{Res}_{\mathbb{Q}}^{K_\beta} C_\beta$. The endomorphism algebra of A_β is given by $M_\beta = \mathbb{Q}(\{\beta(\sigma)\})$, and the representation on the π^n-torsion points of A_β coincides with the representation $\hat{\rho}_{C,\beta,\pi}$ defined earlier.

Let $\epsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ be defined by

$$\epsilon(\sigma) = \beta(\sigma)^2/\deg \mu(\sigma). \tag{1}$$

Then ϵ is a character and

$$\det \hat{\rho}_{C,\beta,\pi} = \epsilon^{-1} \cdot \chi_p, \tag{2}$$

where $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ is the p-adic cyclotomic character.

3. $\mathbb{Q}$-*curves attached to* $a^2 - 2b^6 = c^p$

Let $(a, b, c) \in \mathbb{Z}^3$ be an integer solution to $a^2 - 2b^6 = c^p$ where p is a prime. Consider the associated elliptic curve

$$E : Y^2 = X^3 - 3\sqrt{2}\,(4a + 5\sqrt{2}b^3)\,bX + 4\sqrt{2}\,(a^2 + 7\sqrt{2}ab^3 + 11b^6)$$

with j-invariant

$$j = -432\sqrt{2}\frac{b^3(4a + 5\sqrt{2}b^3)^3}{(a - \sqrt{2}b^3)^3(a + \sqrt{2}b^3)} \tag{3}$$

and discriminant $\Delta = -2^9 \cdot 3^3 \cdot (a - \sqrt{2}b^3)^3 \cdot (a + \sqrt{2}b^3)$.

Lemma 6. *Suppose $a/b^3 \in \mathbb{P}^1(\mathbb{Q})$. Then the j-invariant of E does not lie in $\mathbb{Q}$ except when:*
- *$a/b^3 = 0$ and $j = 54\,000$;*
- *$a/b^3 = \infty$ and $j = 0$.*

Proof. Using (3), we obtain

$$j(a - \sqrt{2}b^3)^3(a + \sqrt{2}b^3) + 432\sqrt{2}b^3(4a + 5\sqrt{2}b^3)^3 = 0.$$

Expanding and equating the coefficients of 1 and $\sqrt{2}$ to 0 yields a system of equations which determines a/b^3 and j, assuming they lie in $\mathbb{P}^1(\mathbb{Q})$. □

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

Otherwise, the j-invariant of E lies in $\mathbb{Q}(\sqrt{2})$. For E to have complex multiplication, its j-invariant must be one of:

- $j = 2417472 \pm 1707264\sqrt{2}$, $d(\mathcal{O}) = -24$;
- $j = 3147421320000 \pm 2225561184000\sqrt{2}$, $d(\mathcal{O}) = -88$.

COROLLARY 7. *E does not have complex multiplication unless:*

- $a/b^3 = 0$, $j = 54000$, $d(\mathcal{O}) = -12$;
- $a/b^3 = \infty$, $j = 0$, $d(\mathcal{O}) = -3$; *or*
- $a/b^3 = \pm 1$, $j = 2417472 \pm 1707264\sqrt{2}$, $d(\mathcal{O}) = -24$.

LEMMA 8. *If $(a, b, c) \in \mathbb{Z}^3$ with $(a, b, c) = 1$ and $a^2 - 2b^6 = c^p$, then either $c = \pm 1$ or c is divisible by a prime not equal to 2 or 3. In the former case, the only possible solutions are $(a, b, c) \in \{(\pm 1, 0, 1), (\pm 1, \pm 1, -1)\}$.*

Proof. The condition $(a, b, c) = 1$ together with inspection of $a^2 - 2b^6$ modulo 3 shows that c is never divisible by 3. A similar reasoning shows that since $p > 1$, c is never divisible by 2. Hence, if c were not divisible by a prime not equal to 2 or 3, it would follow that $c = \pm 1$. Computing the integral points on $a^2 - 2b^6 = \pm 1$ using Magma [2] yields the additional assertion. □

From here on, let us suppose that E arises from a non-trivial proper integer solution to $a^2 - 2b^6 = c^p$, with $c \neq \pm 1$, where p is a prime. Note that a must be odd. Since $a^2 - 2b^6 = (a - \sqrt{2}b^3)(a + \sqrt{2}b^3)$ is not equal to 0 or ± 1, we see that $a - \sqrt{2}b^3$ and $a + \sqrt{2}b^3$ are coprime pth powers up to units, as elements of $\mathbb{Z}[\sqrt{2}]$.

The elliptic curve E is defined over $\mathbb{Q}(\sqrt{2})$. Its conjugate over $\mathbb{Q}(\sqrt{2})$ is 3-isogenous to E over $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ (Magma program isogeny-1.txt). We make a choice of isogenies $\mu(\sigma) : {}^{\sigma}E \to E$ such that $\mu(\sigma) = 1$ for $\sigma \in G_{\mathbb{Q}(\sqrt{2})}$ and $\mu(\sigma)$ is the 3-isogeny above when $\sigma \notin G_{\mathbb{Q}(\sqrt{2})}$.

Let $d(\sigma)$ denote the degree of $\mu(\sigma)$. We have that $d(G_{\mathbb{Q}}) = \{1, 3\} \subseteq \mathbb{Q}^*/\mathbb{Q}^{*2}$. The fixed field K_d of the kernel of $d(\sigma)$ is $\mathbb{Q}(\sqrt{2})$. So $\{2\}$ and $\{3\}$ are dual bases in the terminology of [21, Theorem 3.1]. The quaternion algebra $(2, 3)$ is ramified at 2 and 3. Thus, by [21], a choice of splitting character for $c_E(\sigma, \tau)$ is given by $\epsilon = \epsilon_2\epsilon_3$ where ϵ_2 is the non-trivial character of $\mathbb{Z}/4\mathbb{Z}^{\times}$ and ϵ_3 is the non-trivial character of $\mathbb{Z}/3\mathbb{Z}^{\times}$. The fixed field of ϵ is $K_{\epsilon} = \mathbb{Q}(\sqrt{3})$.

Let $G_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = \{\sigma_1, \sigma_2\}$. We have that

$$\alpha(\sigma_1) = 1,$$
$$\alpha(\sigma_2) = \sqrt{3}.$$

This can be checked by noting that the quotient of ${}^{\sigma_2}E$ by the kernel of the 3-isogeny $\mu(\sigma_2)$ computed using Vélu's formulae multiplies the invariant differential by 1. The resulting quotient elliptic curve is then a twist over $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ of the original E. This twisting multiplies the invariant differential by $\sqrt{3}$.

So now we can express $c_E(\sigma, \tau)$ as $\alpha(\sigma)\,{}^{\sigma}\alpha(\tau)\alpha(\sigma\tau)^{-1}$. Let $\beta(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}$ and $c_{\beta}(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1} \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$. We know from [21] that $c_{\beta}(\sigma, \tau)$ and $c_E(\sigma, \tau)$ represent the same class in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$. The fixed field of β is $K_{\beta} = K_{\epsilon} \cdot K_d = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ and $M_{\beta} = \mathbb{Q}(i, \sqrt{3})$.

Our goal is to find a $\gamma \in \overline{\mathbb{Q}}^*$ so that $c_{\beta}(\sigma, \tau) = \alpha_1(\sigma)\,{}^{\sigma}\alpha_1(\tau)\alpha_1(\sigma\tau)^{-1}$ where $\alpha_1(\sigma) = \alpha(\sigma)\sqrt{{}^{\sigma}\gamma/\gamma}$. Consider the twist E_{β} of E given by the equation

$$E_{\beta} : Y^2 = X^3 - 3\sqrt{2}\,(4a + 5\sqrt{2}b^3)b\gamma^2 X + 4\sqrt{2}\,(a^2 + 7\sqrt{2}ab^3 + 11b^6)\gamma^3. \tag{4}$$

The set of isogenies $\mu_E(\sigma)$ determines a set of isogenies $\mu_{E_{\beta}}(\sigma)$ for E_{β} such that

$$\alpha_{E_{\beta}}(\sigma) = \alpha_E(\sigma)\frac{{}^{\sigma}\sqrt{\gamma}}{\sqrt{\gamma}} = \alpha_1(\sigma)\xi(\sigma).$$

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

Replacing $\mu_{E_\beta}(\sigma)$ by $\mu_{E_\beta}(\sigma)\xi(\sigma)$ gives us a set of isogenies for E_β such that $c_{E_\beta}(\sigma,\tau) = c_\beta(\sigma,\tau)$ as cocycles and not just as classes in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$.

Using a similar technique as for $a^2 + b^{2p} = c^5$ (see [8], where K_β is cyclic quartic), we can make a guess of a possible choice of γ and then verify that it works. We find that $\gamma = -3 + \sqrt{6}$ works. The author has subsequently learned that a similar technique for finding γ also appeared in [11] (where K_β is polyquadratic).

Let $G_{\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}} = \{\sigma_1, \sigma_2, \sigma_3, \sigma_6\}$. We list the resulting values of $\alpha_1(\sigma)$ for convenience (here $z = \sqrt{2} + \sqrt{3}$):

$$\begin{aligned}\alpha_1(\sigma_1) &= 1,\\ \alpha_1(\sigma_2) &= \sqrt{3}z,\\ \alpha_1(\sigma_3) &= z,\\ \alpha_1(\sigma_6) &= \sqrt{3}.\end{aligned}$$

The elliptic curve E_β/K_β is a $\mathbb{Q}$-curve defined over K_β (Magma program isogenyp-1.txt). The discriminant of K_β is $d_{K_\beta/\mathbb{Q}} = 2^8 \cdot 3^2 = 2304$. The prime factorizations of (2) and (3) in K_β are given as follows:

$$\begin{aligned}(2) &= \mathfrak{q}_2^4,\\ (3) &= \mathfrak{q}_3^2.\end{aligned}$$

LEMMA 9. *Suppose that E and E' are elliptic curves defined by*

$$\begin{aligned}E &: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,\\ E' &: Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6',\end{aligned}$$

where the a_i and a_i' lie in a discrete valuation ring $\mathcal{O}$ with uniformizer ν and the Weierstrass equation of E is in minimal form. If $a_i' \equiv a_i \pmod{\nu^8}$, then E' has the same reduction type as E and is also in minimal form.

Proof. Since the Weierstrass equation for E is in minimal form, when E is processed through Tate's algorithm [27], the algorithm terminates at one of steps 1–10 and does not reach step 11 to loop back a second time. Since the transformations used in steps 1–10 are translations, they preserve the congruence $a_i \equiv a_i' \pmod{\nu^8}$ as E and E' are processed through the algorithm; and since the conditions for exiting at steps 1–10 are congruence conditions modulo ν^8 on the coefficients of the Weierstrass equations, we see that if the algorithm applied to E terminates at one of steps 1–10, it must also terminate at the same step for E'. □

LEMMA 10. *Suppose that E and E' are elliptic curves defined by*

$$\begin{aligned}E &: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,\\ E' &: Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6',\end{aligned}$$

where the a_i and a_i' lie in a discrete valuation ring $\mathcal{O}$ with uniformizer ν and the valuation at ν of the discriminants is equal to 12. If E has reduction type II^* and $a_i' \equiv a_i \pmod{\nu^6}$, then E' also has reduction type II^*. If E has reduction type I_0 and $a_i' \equiv a_i \pmod{\nu^6}$, then E' also has reduction type I_0.

Proof. Since the discriminants of E and E' have valuation 12, when E and E' are processed through Tate's algorithm [27], the algorithm terminates at one of steps 1–10 or reaches step 11 to loop back a second time at most once.

If E has reduction type II^*, the algorithm applied to E terminates at step 10. Since the transformations used in steps 1–10 are translations, they preserve the congruence $a_i \equiv a_i' \pmod{\nu^6}$ as E and E' are processed through the algorithm; and since the conditions for exiting at steps 1–10 are congruence conditions modulo ν^6 on the coefficients of the Weierstrass equations, we see that if the algorithm applied to E terminates at step 10, it must also terminate at step 10 for E'.

If E has reduction type I_0, the algorithm applied to E reaches step 11 to loop back a second time and terminate at step 1 (because the valuation of the discriminant of the model for E is equal to 12). Again, since $a_i' \equiv a_i \pmod{\nu^6}$, it follows that the algorithm applied to E' also reaches step 11 to loop back a second time and then terminate at step 1 (again because the valuation of the discriminant of the model for E' is equal to 12). □

THEOREM 11. *The conductor of E_β is*

$$\mathfrak{m} = \mathfrak{q}_2^{16} \cdot \mathfrak{q}_3^{\varepsilon} \prod_{\mathfrak{q} \mid c}{}' \mathfrak{q},$$

where the product does not include primes dividing $2 \cdot 3$ and $\varepsilon = 0$ or 4.

Proof. See tate2m-1.txt, tate3m-1.txt for the computations. Recall that E_β is given by (4) with

$$\Delta_{E_\beta} = -2^9 \cdot 3^3 \cdot (a - \sqrt{2}b^3)^3 \cdot (a + \sqrt{2}b^3) \cdot \gamma^6. \tag{5}$$

Then

$$c_4 = 2^4 \cdot 3^2 \sqrt{2} \cdot b(4a + 5\sqrt{2}b^3) \cdot \gamma^2, \tag{6}$$

$$\begin{aligned} c_6 &= -2^7 \cdot 3^3 \sqrt{2} \cdot (a^2 + 7\sqrt{2}ab^3 + 11b^6) \cdot \gamma^3 \qquad (7)\\ &= -2^7 \cdot 3^3 \sqrt{2} \cdot (a + \tfrac{1}{4}(-7z^3 - 3z^2 + 63z + 15)b^3)(a + \tfrac{1}{4}(-7z^3 + 3z^2 + 63z - 15)b^3) \cdot \gamma^3. \end{aligned}$$

Let $\mathfrak{q}$ be a prime not dividing $2 \cdot 3$ but dividing Δ_{E_β}. The elliptic curve E_β has multiplicative bad reduction at $\mathfrak{q}$ if one of $c_4, c_6 \not\equiv 0 \pmod{\mathfrak{q}}$. Since γ is not divisible by $\mathfrak{q}$ and $(a, b) = 1$, we note that $c_4 \equiv c_6 \equiv 0 \pmod{\mathfrak{q}}$ happens if and only if

$$b^3 \equiv 0 \pmod{\mathfrak{q}} \quad \text{or} \quad 4a + 5\sqrt{2}b^3 \equiv 0 \pmod{\mathfrak{q}}$$

and

$$a + \tfrac{1}{4}(-7z^3 - 3z^2 + 63z + 15)b^3 \equiv 0 \pmod{\mathfrak{q}}$$

or

$$a + \tfrac{1}{4}(-7z^3 + 3z^2 + 63z - 15)b^3 \equiv 0 \pmod{\mathfrak{q}}.$$

The determinants of the resulting linear system in the variables a and b^3 in all four cases are only divisible by primes above 2 and 3. Hence E_β has multiplicative bad reduction at $\mathfrak{q}$.

Over the prime 2, the test cases in each congruence class modulo ν_2^8 are in minimal form and the reduction type is II^*, I_4^* or I_{12}^*, so we use Lemma 9. We note that once the reduction type is known and the conductor is known, the valuation of the discriminant is determined (this will be used later to obtain information about the images of inertia at $\mathfrak{q}_2$). Over the prime 3, the valuation of the discriminant of E_β is 12 and the reduction type is II^* or I_0, so we use Lemma 10 by testing cases modulo ν_3^6. □

THEOREM 12. *The conductor of $\mathrm{Res}_{\mathbb{Q}}^{K_\beta} E_\beta$ is*

$$d_{K_\beta/\mathbb{Q}}{}^2 \cdot N_{K_\beta/\mathbb{Q}}(\mathfrak{m}) = 2^{32} \cdot 3^{4+2\varepsilon} \cdot \prod_{q \mid c}{}' q^4,$$

where the product does not include primes dividing $2 \cdot 3$ and $\varepsilon = 0$ or 4.

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

Proof. This follows from [19, Lemma, p. 178] and the fact discussed there that the ℓ-adic representation of a restriction of scalars is the induced representation of the ℓ-adic representation of the given abelian variety. □

Let $A = \mathrm{Res}_{\mathbb{Q}}^{K_\beta} E_\beta$. By [21, Theorem 5.4], A is an abelian variety of GL_2-type with $M_\beta = \mathbb{Q}(i, \sqrt{3})$. The conductor of the system of $M_{\beta,\pi}[G_{\mathbb{Q}}]$-modules $\{\hat{V}_\pi(A)\}$ is given by

$$N = 2^8 \cdot 3^{1+\varepsilon/2} \cdot \prod_{q|c}{}' q, \tag{8}$$

using the conductor results explained in [8].

This means, by the usual arguments (whose main components we briefly outline below), that $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$, where g is a newform in $S_2(\Gamma_0(M), \epsilon^{-1})$ and $M = 768$ or $M = 6912$.

For the next two theorems, it is useful to recall that $a - \sqrt{2}b^3$ and $a + \sqrt{2}b^3$ are coprime pth powers up to units in $\mathbb{Z}[\sqrt{2}]$.

THEOREM 13. *The representation $\phi_{E,p|_{I_p}}$ is finite flat for $p \neq 2, 3$.*

Proof. This follows from the fact that E has good or multiplicative bad reduction at primes above p when $p \neq 2, 3$, and that in the case of multiplicative bad reduction, the exponent of a prime above p in the minimal discriminant of E is divisible by p. Also, p is unramified in K_β so that $I_p \subseteq G_{K_\beta}$. □

THEOREM 14. *The representation $\phi_{E,p|_{I_\ell}}$ is trivial for $\ell \neq 2, 3, p$.*

Proof. This follows from the fact that E has good or multiplicative bad reduction at primes above ℓ when $\ell \neq 2, 3$, and that in the case of multiplicative bad reduction, the exponent of a prime above ℓ in the minimal discriminant of E is divisible by p. Also, ℓ is unramified in K_β so that $I_\ell \subseteq G_{K_\beta}$. □

THEOREM 15. *Suppose $p \neq 2, 3$. The conductor of $\rho = \rho_{E,\beta,\pi}$ is either 768 or 6912.*

Proof. Suppose $\ell \neq 2, 3, p$. Since $\ell \neq 2, 3$, we see that K_β is unramified at ℓ and hence G_{K_β} contains I_ℓ. Now, in our case, $\rho_{|G_{K_\beta}}$ is isomorphic to $\phi_{E,p}$. Since $\phi_{E,p|_{I_\ell}}$ is trivial, we have that $\rho_{|_{I_\ell}}$ is trivial and so ρ is unramified outside $\{2, 3, p\}$.

Suppose $\ell = 2, 3$. The representation $\hat{\phi}_{E,p|_{I_\ell}}$ factors through a finite group of order divisible only by the primes 2 and 3. Now, in our case, $\hat{\rho}_{|G_{K_\beta}}$ is isomorphic to $\hat{\phi}_{E,p}$. Hence, the representation $\hat{\rho}_{|_{I_\ell}}$ also factors through a finite group of order divisible only by the primes 2 and 3. It follows that the exponent of ℓ in the conductor of ρ is the same as in the conductor of $\hat{\rho}$ as $p \neq 2, 3$. □

PROPOSITION 16. *Suppose $p \neq 2, 3$. Then the weight of $\rho = \rho_{E,\beta,\pi}$ is 2.*

Proof. The weight of ρ is determined by $\rho_{|_{I_p}}$. Since $p \neq 2, 3$, we see that K_β is unramified at p and hence G_{K_β} contains I_p. Now, in our case, $\rho_{|G_{K_\beta}}$ is isomorphic to $\phi_{E,p}$. Since $\phi_{E,p|_{I_p}}$ is finite flat and its determinant is the pth cyclotomic character, we have that the weight of ρ is 2 (see [25, Proposition 4]). □

PROPOSITION 17. *The character of $\rho_{E,\beta,\pi}$ is $\epsilon^{-1} = \epsilon$.*

Proof. This follows from (2). □

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

THEOREM 18. *Suppose that the representation* $\rho_{E,\beta,\pi}$ *is reducible for* $p \neq 2, 3, 5, 7, 13$. *Then* E *has potentially good reduction at all primes above* $\ell > 3$.

Proof. See [**12**, Proposition 3.2]. We note that the results still apply even though the isogeny between E and its conjugate is only defined over $\mathbb{Q}(\sqrt{3}, \sqrt{2})$; see [**8**]. □

COROLLARY 19. *The representation* $\rho_{E,\beta,\pi}$ *is irreducible for* $p \neq 2, 3, 5, 7, 13$.

Proof. This follows from Theorem 18, the formula (3) for the j-invariant of E, and Lemma 8. □

Assuming that $\rho_{E,\beta,\pi}$ is irreducible (which holds for $p \neq 2, 3, 5, 7, 13$ by Corollary 19), $\rho_{E,\beta,\pi}$ is modular because of the validity of Serre's conjecture [**14–16, 25**]. By Serre's refined conjecture (cf. [**23**]), as applied to $\rho_{E,\beta,\pi}$, it follows that $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$ for some newform in $S_2(\Gamma_0(M), \epsilon^{-1})$, where $M = 768$ or 6912.

Additionally, we have that $\hat{\rho}_{E,\beta,\pi} \cong \hat{\rho}_{f,\pi}$ for some newform $f \in S_2(\Gamma_0(N), \epsilon^{-1})$, where $\hat{\rho}_{f,\pi}$ is the π-adic Galois representation attached to f (cf. [**25**, § 4.7]). From formula (1) for β, we deduce that

$$a_q(f) \in \begin{cases} \mathbb{Z} & \text{if } \epsilon(q) = 1, \mu(q) = 1, \\ \mathbb{Z} \cdot i & \text{if } \epsilon(q) = -1, \mu(q) = 1, \\ \mathbb{Z} \cdot \sqrt{3} & \text{if } \epsilon(q) = 1, \mu(q) = -1, \\ \mathbb{Z} \cdot \sqrt{3}i & \text{if } \epsilon(q) = -1, \mu(q) = -1, \end{cases} \tag{9}$$

where $\mu = (\frac{8}{\cdot})$ is the quadratic character associated to $\mathbb{Q}(\sqrt{2})$.

Let D_q and I_q denote the decomposition and inertia groups of $G_{\mathbb{Q}}$ over the prime q.

THEOREM 20. *Let* $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N), \psi)$ *be a newform.*

(i) *The conductor of* $\{\hat{\rho}_{f,\pi}\}$ *is equal to* N.

(ii) *Suppose* $q \neq p$ *and* $q \,||\, N$.

If q *does not divide the conductor of* ψ, *then* $\hat{\rho}_{f,\pi}\,|_{D_q}$ *is of the form*

$$\begin{pmatrix} \chi\chi_p & * \\ 0 & \chi \end{pmatrix}.$$

If q *divides the conductor of* ψ, *then* $\hat{\rho}_{f,\pi}\,|_{D_q}$ *is of the form*

$$\begin{pmatrix} \chi^{-1}\chi_p\psi & 0 \\ 0 & \chi \end{pmatrix}.$$

Here χ *is the unramified character of* D_q *which sends* Frob_q *to* a_q, $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ *is the* p*-adic cyclotomic character, and we regard* ψ *as a Galois character.*

Proof. See [**6**, Théorème 2.1], [**7**, Théorème (A)], [**10**, Theorem 3.1] and [**13**, (0.1)]. □

Suppose that K_g is not contained in $\mathbb{Q}(i, \sqrt{3})$. Let $q \neq 2, 3$ be a prime such that $a_q(g) \notin \mathbb{Q}(i, \sqrt{3})$. Assume that $p \neq q$. Then we have that

$$\begin{aligned} p \mid N_{L/\mathbb{Q}}\big(a_q(g)^2 - \epsilon^{-1}(q)(q+1)^2\big) \quad & \text{if } q \mid c, \\ p \mid N_{L/\mathbb{Q}}\big(a_q(g) - a_q(f)\big) \quad & \text{if } q \nmid c, \end{aligned}$$

where L is the compositum of K_g and $\mathbb{Q}(i, \sqrt{3})$. This follows from the isomorphism $\rho_{E,\beta,\pi} \cong \rho_{f,\pi} \cong \rho_{g,\pi}$ and comparing traces of $\rho_{g,\pi}$ and $\rho_{f,\pi}$ on a Frobenius element Frob_q. For instance, in the former case, we have that $\mathrm{tr}\, \rho_{g,\pi}(\mathrm{Frob}_q) = a_q(g)$, and $\mathrm{tr}\, \rho_{f,\pi} = a_q(f)(q+1)$ by Theorem 20. From [**20**, Theorem 4.6.17], we have that $a_q(f)^2 = \epsilon^{-1}(q)$, so the result follows by taking norms of the difference of squares of the traces.

In the latter case, we also note that $a_q(f)$ is restricted by the properties of inner twist above (9) and also by the fact that $|a_q(f)| < 2\sqrt{q}$. Hence, for each such prime q, we obtain that p is restricted to lie in a finite subset of primes because $a_q(g) \neq a_q(f)$. Taking the intersection of these subsets for different q further restricts the possibilities for the prime p.

There are ten Galois conjugacy classes of newforms $F_1, \ldots, F_{10}$ in $S_2(\Gamma_0(768), \epsilon^{-1})$; see inner-768.txt. By cm-768.txt we find that F_8 has CM by -3; F_3, F_6 and F_7 have CM by -8; and F_9 and F_{10} have CM by -24. The field of coefficients of the remaining forms F_1, F_2, F_4 and F_5 is equal to $\mathbb{Q}(\sqrt{2})$, which is not contained in $\mathbb{Q}(i, \sqrt{3})$. In fact, only F_8 and F_9 have field of coefficients contained in $\mathbb{Q}(i, \sqrt{3})$. For those forms with K_g not contained in $\mathbb{Q}(i, \sqrt{3})$, we obtain a bound of $p \in \{2, 3, 5, 17, 23\}$ from bound-768.txt.

There are 21 Galois conjugacy classes of newforms $G_1, \ldots, G_{21}$ in $S_2(\Gamma_0(6912), \epsilon^{-1})$; see inner-6912.txt. From cm-6912.txt we find that G_1 and G_2 have CM by -3, while G_{17} and G_{18} have CM by -24. Moreover:

G_3 arises from the solution $a = 12, b = -2$;
G_5 arises from the solution $a = 12, b = 2$;
G_4 arises from the solution $a = 2, b = 1$;
G_6 arises from the solution $a = 2, b = -1$.

The above statements can be verified by noting that these near solutions give rise to a form at level 6912 and by counting the number of points modulo primes which split completely in K_β. It turns out that we only need to consider such primes (which is convenient for computation) to identify which of the G_i correspond to the above solutions; see countE-1.txt.

Let E_i be the corresponding $\mathbb{Q}$-curve (namely, the E_β) which is attached to the solution in each of the cases $i = 3, 5, 4, 6$. Each $\rho_{G_i,\pi}|_{G_{K_\beta}} \cong \phi_{E_i,\ell}$ for $i = 3, 5, 4, 6$. There is no twisting as β is trivial on G_{K_β}. Let $I_{\mathfrak{q}_2}$ denote the inertia group at $\mathfrak{q}_2$ of K_β. One can compute that $\phi_{E_i,\ell}(I_{\mathfrak{q}_2})$ is divisible by 3 using [**17**, Théorème 3] for $i = 3, 5, 4, 6$, because the valuation of the minimal discriminant at $\mathfrak{q}_2$ of E_i is not divisible by 3 (see output from tate2m-1.txt).

On the other hand, we note that we cannot have $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$ in the equation $a^2 - 2b^6 = c^p$ as $p > 1$. Using [**17**, Théorème 3], we compute that $\phi_{E,\ell}(I_{\mathfrak{q}_2})$ is not divisible by 3 when $a \equiv 1 \pmod 2$ and $b \equiv 0, 1 \pmod 2$ because the valuation of the minimal discriminant at $\mathfrak{q}_2$ of E_β in these cases is divisible by 3 (see output from tate2m-1.txt). Hence, g cannot be any one of the G_i for $i = 3, 5, 4, 6$. The field of coefficients of the remaining forms $G_7, \ldots, G_{21}$ is not contained in $\mathbb{Q}(i, \sqrt{3})$. For those forms with K_g not contained in $\mathbb{Q}(i, \sqrt{3})$, we obtain a bound of $p \in \{2, 3, 5, 7, 11, 13, 17\}$; see bound-6912.txt.

THEOREM 21. *Suppose that the representation $\rho_{E,\beta,\pi}$ has image lying in the normalizer of a split Cartan subgroup for $p \neq 2, 3, 5, 7, 13$. Then E has potentially good reduction at all primes above $\ell > 3$.*

Proof. See [**12**, Proposition 3.4]. We note that the results still apply even though the isogeny between E and its conjugate is only defined over $\mathbb{Q}(\sqrt{3}, \sqrt{2})$; see [**8**]. □

COROLLARY 22. *The representation $\rho_{E,\beta,\pi}$ does not have image lying in the normalizer of a split Cartan subgroup for $p \neq 2, 3, 5, 7, 13$.*

Proof. This follows from Theorem 21, formula (3) for the j-invariant of E, and Lemma 8. □

For p to be split in the quadratic order of discriminant -24, we must have that $p \equiv 1, 5, 7, 11 \pmod{24}$. Similarly, p splits in the quadratic order of discriminant -3 if and only if $p \equiv 1 \pmod 6$.

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

Proof of Theorem 1. If $p \notin \{2,3,5,7,13\} \cup \{2,3,5,7,11,13,17,23\}$, then we must have that $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$ where $g = F_9$ has complex multiplication by $\mathbb{Q}(\sqrt{-24})$, or $g = F_8, G_1, G_2$, which have complex multiplication by $\mathbb{Q}(\sqrt{-3})$. If $p \equiv 1, 7 \pmod{24}$, then p splits in both $\mathbb{Q}(\sqrt{-24})$ and $\mathbb{Q}(\sqrt{-3})$, forcing $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$ to have image lying in the normalizer of a split Cartan subgroup, a contradiction to Ellenberg's results.

Concerning the latter fact about the image, we give some details. We are given that g has complex multiplication by $F = \mathbb{Q}(\sqrt{-24})$ or $\mathbb{Q}(\sqrt{-3})$ in the sense that $a_q(g)\phi(q) = a_q(g)$ for all but finitely many primes q, where ϕ is the quadratic Dirichlet character associated to F. By [26], A_g is isogenous over $\overline{\mathbb{Q}}$ to the power of an elliptic curve C with complex multiplication by F, which we shall take to be E as defined previously. Hence, A_g is an abelian variety of GL_2-type defined over $\mathbb{Q}$ attached to C. We have shown that A_g is isogenous over $\mathbb{Q}$ to A_β for some splitting map β for $c_C(\sigma,\tau)$. However, we know that $\det \hat{\rho}_{g,\pi} = \epsilon^{-1}\chi_p$, so the splitting character ϵ_β equals ϵ. It follows that β is the β defined previously, up to multiplication by a quadratic Galois character unramified outside $\{2,3\}$. Thus, K_β is unramified outside $\{2,3\}$. We may now take the field of definition of the isogeny between A_g and C^2 to be K_β by the construction of A_β. Let $L = K_\beta \cdot F$. There is an injection of $M = F \cdot K_g$ into the endomorphism algebra of A_g defined over L, and $\hat{V}_p(A_g) \cong M \otimes \mathbb{Q}_p$ as G_L-modules. Since $p \equiv 1, 7 \pmod{24}$, p is split in F and so $\rho_{g,\pi}|_{G_L}$ has image lying in a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. This implies that, in fact, $\mathbb{P}\rho_{g,\pi}|_{G_F}$ has image lying in a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. This is because we know that $\rho_{g,\pi}|_{G_F}$ is abelian [22, Proposition 4.4], so if $\mathbb{P}\rho_{g,\pi}|_{G_F}$ does not lie in a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, then it must lie in a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Therefore $\mathbb{P}\rho_{g,\pi}|_{G_L}$ lies in the center of $\mathrm{GL}_2(\mathbb{F}_p)$, implying further that $\det \rho_{g,\pi}|_{G_L}$ lies in the subgroup of squares of $\mathbb{F}_p^\times$. However, $\det \rho_{g,\pi}|_{G_L} = \overline{\epsilon}^{-1}\overline{\chi}_p$ is surjective to $\mathbb{F}_p^\times$ since L does not contain a primitive pth root of unity for $p > 3$. Finally, as $[G_\mathbb{Q} : G_F] = 2$, it follows that $\mathbb{P}\rho_{g,\pi}$ itself has image lying in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ by the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. □

We note the near solutions

$$33^2 - 2 \cdot 2^6 = 31^2,$$
$$71^2 - 2 \cdot 2^6 = 17^3.$$

However, from the point of view of the method, these near solutions do not cause trouble because they do not give rise to modular forms at the minimal level (which can sometimes happen).

4. *Eliminating the newforms F_8, G_1 and G_2 for the equation $a^2 - 2 = c^p$*

The equation $a^2 - 2b^6 = c^p$ has two obstructive solutions: $(\pm 1, 0, 1)$, which gives rise to G_1, and $(\pm 1, \pm 1, -1)$, which gives rise to F_9. If we are only interested in the equation $a^2 - 2 = c^p$, then the solution $(\pm 1, 0, 1)$ does not pose an obvious obstruction.

Let $b = 1$. Recall that $E = E_{a,b} = E_a$ is given by

$$E : Y^2 = X^3 - 3\sqrt{2}\,(4a + 5\sqrt{2}b^3)bX + 4\sqrt{2}\,(a^2 + 7\sqrt{2}ab^3 + 11b^6).$$

Let $E' = E'_{a,b} = E'_a$ be the elliptic curve

$$E' : Y^2 = X^3 + 2aX^2 + 2b^pX,$$

which is a Frey elliptic curve over $\mathbb{Q}$ for the equation $a^2 - 2b^p = c^p$.

We will show how to eliminate the cases of $g = F_8, G_1, G_2$ by using a combination of congruences from the two Frey curves E and E'. This is an example of the multi-Frey technique [3, 5] as applied to the situation where one of the Frey curves is a $\mathbb{Q}$-curve. We

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

thank S. Siksek for suggesting Lemma 24, which allows one to apply the multi-Frey technique to our situation.

Applying the modular method with E' as the Frey curve shows that $\rho_{E',\pi} \cong \rho_{g',\pi}$ for some newform $g' \in S_2(\Gamma_0(128))$ (see [9, § 15.7.1]), under the assumption that $b = 1$. The possible forms g' were computed using b32-modformagain.txt. The reason the multi-Frey method works is that the near solution $(\pm 1, 0, 1)$ corresponds to a singular E' and so this solution does not pose an obstruction from the point of view of the Frey curve E'. By linking the two Frey curves E and E', it is possible to pass this information from the Frey curve E' to the Frey curve E using the multi-Frey technique.

The following lemma results from the condition $\rho_{E',\pi} \cong \rho_{g',\pi}$ and standard modular method arguments.

LEMMA 23. *Let $q \geqslant 5$ be prime and assume $q \neq p$, where $p \geqslant 5$ is a prime. Let*

$$C_\alpha(q, g') = \begin{cases} a_q(E'_\alpha) - a_q(g') & \text{if } x^2 - 2 \not\equiv 0 \pmod{q}, \\ (q+1)^2 - a_q(g')^2 & \text{if } x^2 - 2 \equiv 0 \pmod{q}. \end{cases}$$

If $a \equiv \alpha \pmod{q}$, then $p \mid C_\alpha(q, g')$.

Proof. See [9, § 15.7.1] for details on showing $\rho_{E',\pi} \cong \rho_{g',\pi}$. □

For our choice of splitting map β, we attached a Galois representation $\rho_{E,\beta,\pi}$ to E such that $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$ for some newform $g \in S_2(\Gamma_0(M), \epsilon)$ where $M = 768$ or 6912. We wish to eliminate the cases of $g = F_8, G_1, G_2$. The following is the analog of Lemma 23 for $E = E_{a,b}$.

LEMMA 24. *Let $q \geqslant 5$ be prime and assume $q \neq p$, where $p \neq 2, 3, 5, 7, 13$ is a prime. Let*

$$B_\alpha(q, g) = \begin{cases} N(a_q(E_\alpha)^2 - \epsilon(q) a_q(g)^2) & \text{if } x^2 - 2 \not\equiv 0 \pmod{q} \text{ and } \left(\frac{2}{q}\right) = 1, \\ N(a_q(g)^2 - a_{q^2}(E_\alpha) - 2q\epsilon(q)) & \text{if } x^2 - 2 \not\equiv 0 \pmod{q} \text{ and } \left(\frac{2}{q}\right) = -1, \\ N(\epsilon^{-1}(q)(q+1)^2 - a_q(g)^2) & \text{if } x^2 - 2 \equiv 0 \pmod{q}, \end{cases}$$

where $a_{q^i}(E_\alpha)$ is the trace of Frob_q^i acting on the Tate module $T_p(E_\alpha)$ and $N(\cdot)$ is the norm from the coefficient field of g down to $\mathbb{Q}$.

If $a \equiv \alpha \pmod{q}$, then $p \mid B_\alpha(q, g)$.

Proof. Recall the set-up in Sections 2 and 3. Let π be a prime of M_β above p. The mod π representation $\rho_{A_\beta,\pi}$ of $G_\mathbb{Q}$ attached to A_β is related to E_β by

$$\mathbb{P}\rho_{A_\beta,\pi}|_{G_K} \cong \mathbb{P}\phi_{E_\beta,p},$$

where $\phi_{E_\beta,p}$ is the representation of G_K on the p-adic Tate module $T_p(E_\beta)$ of E_β, and the $\mathbb{P}$ means that we consider isomorphism up to scalars. The algebraic formula which describes $\rho_{E_\beta,\beta,\pi} = \rho_{A_\beta,\pi} \cong \rho_{f,\pi}$ is

$$\rho_{A_\beta,\pi}(\sigma)(1 \otimes x) = \beta(\sigma)^{-1} \otimes \mu'_\beta(\sigma)(\phi_{E_\beta,p}(\sigma)(x))$$

where $1 \otimes x \in M_{\beta,\pi} \otimes T_p(E_\beta)$. Here, $\mu'_\beta(\sigma)$ is the chosen isogeny from ${}^\sigma E_\beta \to E_\beta$ for each σ which is constant on G_K (see the paragraph after equation (4)). Let $\mu'_\beta(\sigma) = \mu_{E_\beta}(\sigma)\xi(\sigma)$.

If $x^2 - 2 \equiv 0 \pmod{q}$, then $q \mid c$. Recall that the conductor of A_β is given by

$$2^4 \cdot 3^{1+\varepsilon/2} \cdot \prod_{q \mid c}' q,$$

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

so that q exactly divides the conductor of A_β. It follows from [6, Théorème 2.1], [7, Théorème (A)], [10, Theorem 3.1], [13, (0.1)] and the fact that $\rho_{f,\pi} \cong \rho_{g,\pi}$ that

$$p \mid N(a_q(g)^2 - \epsilon^{-1}(q)(q+1)^2).$$

For further details, see Theorem 20 and the paragraph after it. The condition $p \neq 2, 3, 5, 7, 13$ is needed to ensure the irreducibility of $\rho_{E,\beta,\pi} \cong \rho_{f,\pi}$.

If $x^2 - 2 \not\equiv 0 \pmod q$, then let $\mathfrak{q}$ be a prime of K_β over q. Since $a \equiv \alpha \pmod q$ and $\mathfrak{q}$ is a prime of good reduction, $a_q(E) = a_q(E_\alpha)$.

We now wish to relate the representation $\rho_{E_\beta,\beta,\pi} = \rho_{A_\beta,\pi} \cong \rho_{f,\pi}$ to the representation $\phi_{E,p}$ for the original E. We know that

$$\begin{aligned} c_{E_\beta}(\sigma,\tau) &= \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}, \\ c_{E_\beta}(\sigma,\tau) &= c_E(\sigma,\tau)\kappa(\sigma)\kappa(\tau)\kappa(\sigma\tau)^{-1}, \end{aligned}$$

where $\kappa(\sigma) = {}^{\sigma}\sqrt{\gamma}/\sqrt{\gamma}$ and $\gamma = -3 + \sqrt{6}$. It follows that

$$c_E(\sigma,\tau) = \beta'(\sigma)\beta'(\tau)\beta'(\sigma\tau)^{-1},$$

where $\beta'(\sigma) = \beta(\sigma)\kappa(\sigma)$ so that β' is a splitting map for the original cocycle $c_E(\sigma,\tau)$. Also, recall that $\epsilon(\mathrm{Frob}_q) = (\frac{12}{q})$.

Now we have that

$$\rho_{A_{\beta'},\pi}(\sigma)(1 \otimes x) = \beta'(\sigma)^{-1} \otimes \mu_E(\sigma)(\phi_{E,p}(\sigma)(x)),$$

where $1 \otimes x \in M_{\beta,\pi} \otimes T_p(E)$. For this choice of $\beta'(\sigma)$, we have that $\rho_{A_{\beta'},\pi} \cong \kappa(\sigma)\xi(\sigma) \otimes \rho_{A_\beta,\pi} \cong \kappa(\sigma)\xi(\sigma) \otimes \rho_{f,\pi}$. This can be seen by fixing the isomorphism $\iota: E \cong E_\beta$ using standard Weierstrass models and then using the following commutative diagram (μ_{E_β} is defined by this diagram).

$$\begin{array}{ccccc} E_\beta & \xrightarrow{\ \sigma\ } & {}^{\sigma}E_\beta & \xrightarrow{\ \mu_{E_\beta}(\sigma)\ } & E_\beta \\ \uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle {}^{\sigma}\iota} & & \uparrow{\scriptstyle \iota} \\ E & \xrightarrow{\ \sigma\ } & {}^{\sigma}E & \xrightarrow{\ \mu_E(\sigma)\ } & E \end{array}$$

Recall that $\beta(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}$ so that $\beta'(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}\kappa(\sigma)$. We note that $d(\sigma) = 1$ if $\sigma \in G_{\mathbb{Q}(\sqrt{2})}$ and $d(\sigma) = 3$ if $\sigma \notin G_{\mathbb{Q}(\sqrt{2})}$.

Now $(\frac{2}{q}) = 1$ means that $\sigma = \mathrm{Frob}_q \in G_{\mathbb{Q}(\sqrt{2})}$. If $\sigma \in G_{\mathbb{Q}(\sqrt{2})}$, then $\mu_E(\sigma) = \mathrm{id}$ and $d(\sigma) = 1$, so $\rho_{A_{\beta'},\pi}(\sigma)(1 \otimes x) = \beta'(\sigma)^{-1} \otimes \mu_E(\sigma)(\phi_{E,p}(\sigma)(x)) = \sqrt{\epsilon(\sigma)}^{-1}\kappa(\sigma)^{-1} \otimes \phi_{E,p}(\sigma)(x)$ and hence $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma) = \sqrt{\epsilon(\sigma)}^{-1}\kappa(\sigma)^{-1} \cdot \mathrm{tr}\,\phi_{E,p}(\sigma)$ and $\epsilon(q)a_q(f)^2 = a_q(E)^2$. Since $a_q(f) \equiv a_q(g) \pmod \pi$, we have that $p \mid B_\alpha(q,g)$ in the case where $(\frac{2}{q}) = 1$.

If $(\frac{2}{q}) = -1$, then $\sigma = \mathrm{Frob}_q \notin G_{\mathbb{Q}(\sqrt{2})}$. But then $\sigma^2 \in G_{\mathbb{Q}(\sqrt{2})}$ and, in fact, $\sigma^2 \in G_{\mathbb{Q}(\sqrt{2},\sqrt{3})}$, so by the above argument we get that $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma^2) = \sqrt{\epsilon(\sigma)}^{-1}\kappa(\sigma)^{-1} \cdot \mathrm{tr}\,\phi_{E,p}(\sigma^2) = \mathrm{tr}\,\phi_{E,p}(\sigma^2) = a_{q^2}(E)$. Also, $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma) = \kappa(\sigma)\xi(\sigma)a_q(f)$ and so $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma)^2 = a_q(f)^2$. We have that

$$\begin{aligned} \frac{1}{\det(1 - \rho_{A_{\beta'},\pi}(\sigma)q^{-s})} &= \exp \sum_{r=1}^{\infty} \mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma^r)\frac{q^{-sr}}{r} \\ &= \frac{1}{1 - \mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma)q^{-s} + q\epsilon(q)q^{-2s}}. \end{aligned}$$

The determinant and traces are of vector spaces over $M_{\beta,\pi}$. Computing the coefficient of q^{-2s} and equating, we get that $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma^2) = \mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma)^2 - 2q\epsilon(q)$; so, in the end, $a_q(f)^2 - 2q\epsilon(q) = a_{q^2}(E)$. Since $a_q(f) \equiv a_q(g) \pmod \pi$, we have that $p \mid B_\alpha(q,g)$ in the case where $(\frac{2}{q}) = -1$ as well. □

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

Let

$$A_q(g,g') := \prod_{\alpha\in\mathbb{F}_q} \gcd(B_\alpha(q,g), C_\alpha(q,g')).$$

Then we must have that $p \mid A_q(g,g')$. For a pair g, g', we can pick a prime q and compute $A_q(g,g')$. Whenever this $A_q(g,g') \neq 0$, we obtain a bound on p so that the pair g, g' cannot arise for p larger than this bound.

For $g = F_8, G_1, G_2$ and g' running through the newforms in $S_2(\Gamma_0(128))$, the above process eliminates all possible pairs $g = F_8, G_1, G_2$ and g'. In particular, using $q = 5$ for each pair shows that $p \in \{2,3\}$. Hence, if $p \notin \{2,3,5\}$, then $g = F_8, G_1, G_2$ is not possible. In fact, applying the multi-Frey method to all forms except $g = F_9$ gives a bound of $p \in \{2,3,5\}$ using the primes $q = 5, 7$ (see multi-frey-1.txt). Hence, under the restriction $b = 1$ and $p \neq 2, 3, 5, 7, 13$, the only form that remains to be eliminated is $g = F_9$, which can be done if $p \equiv 1, 5, 7, 11 \pmod{24}$ (see the proof of Theorem 1). This establishes Theorem 5.

5. *Congruence restrictions obtained from the multi-Frey method*

Although it is not possible to eliminate the form $g = F_9$ for p inert in $\mathbb{Q}(\sqrt{-24})$, it is still possible to obtain good congruence restrictions on the possible solutions (a, c). Indeed, for $q \geqslant 5$, we can run through all possible $\alpha \in \mathbb{F}_q$. If $\gcd(B_\alpha(q,g), C_\alpha(q,g')) \neq 0$ for all g', then this restricts p to a finite number of possibilities. Otherwise, $a \equiv \alpha \pmod{q}$ is possible.

It turns out that for some primes $q \geqslant 5$, this method shows that either $a \equiv \pm 1 \pmod{q}$ or p is among a finite list of possibilities. For example, taking $q = 5$ shows that $a \equiv \pm 1 \pmod{5}$ or $p \in \{2,3\}$.

We have computed with b32-cong.txt all primes $5 \leqslant q \leqslant 1000$ such that:

- the prime factors of $q - 1$ are less than or equal to 37;
- the above method shows that either $a \equiv \pm 1 \pmod{q}$ or $p \leqslant 37$.

The list of such primes q is given by

$$\begin{aligned} S = \{&5, 7, 11, 13, 19, 23, 29, 31, 37, 41, 61, 67, 73, 89, 113, 127, 137, 149, 181, 191,\\ &193, 197, 223, 233, 251, 257, 349, 373, 379, 421, 457, 461, 521, 547, 599, 617,\\ &661, 677, 701, 761, 769, 811, 829, 881, 883, 953\}. \end{aligned} \tag{10}$$

As a result of this computation, we obtain the following corollary.

Corollary 25. *If $a^2 - 2 = c^p$ where $a, c \in \mathbb{Z}$, $p \geqslant 5$ is prime and $c \neq -1$, then $c > 10^{102}$.*

Proof. The equation $a^2 - 2 = c^p$ has been solved for $5 \leqslant p \leqslant 37$, so let us assume $p > 37$. For $q \in S$, we can thus conclude that $a \equiv \pm 1 \pmod{q}$. Hence $c^p \equiv -1 \pmod{q}$. But $p \nmid q - 1$, as the only prime divisors of $q - 1$ are less than or equal to 37, so that $c \equiv -1 \pmod{q}$ for every $q \in S$. Let $Q = \prod_{q\in S} q$. Then $c \equiv -1 \pmod{Q}$. If $c \neq -1$, then $c > 0$ and so $c \geqslant -1 + Q > 10^{102}$. □

Acknowledgements. I would like to thank M. Bennett and S. Siksek for useful suggestions and discussions pertaining to this paper, and the referee for carefully reading and providing a detailed list of useful suggestions and corrections to the text and programs.

References

1. M. Bennett and I. Chen, 'Multi-frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^p$', *Algebra Number Theory*, to appear.
2. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–265.

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press

3. Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, 'Almost powers in the Lucas sequences', *J. Théor. Nombres Bordeaux* 20 (2008) 555–600.
4. Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers', *Ann. of Math.* (2) 163 (2006) 969–1018.
5. Y. Bugeaud, M. Mignotte and S. Siksek, 'A multi-Frey approach to some multi-parameter families of Diophantine equations', *Canad. J. Math.* 60 (2008) 491–519.
6. H. Carayol, 'Sur les représentations attachés aux forms modulaire de Hilbert', *C. R. Acad. Sci. Paris Série I* 196 (1983) 629.
7. H. Carayol, 'Sur les représentations p-adiques associées aux forms modulaire de Hilbert', *Ann. Sci. Éc. Norm. Supér.* 19 (1986) 409–468.
8. I. Chen, 'On the equation $a^2 + b^{2p} = c^5$', *Acta Arith.* 143 (2010) 345–375.
9. H. Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics 240 (Springer, New York, 2007).
10. H. Darmon, F. Diamond and R. Taylor, 'Fermat's last theorem', *Elliptic curves, modular forms & Fermat's Last Theorem (Hong Kong, 1993)* (International Press, Cambridge, MA, 1997) 2–140.
11. L. Dieulefait and J. J. Urroz, 'Solving Fermat-type equations $x^4 + dy^2 = z^p$ via modular $\mathbb{Q}$-curves over polyquadratic fields', *J. reine angew. Math* 633 (2009) 183–195.
12. J. Ellenberg, 'Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$', *Amer. J. Math.* 126 (2004) 763–787.
13. B. H. Gross, 'A tameness criterion for Galois representations associated to modular forms (mod p)', *Duke Math. J.* 61 (1990) 445–517.
14. C. Khare and J.-P. Wintenberger, 'Serre's modularity conjecture (I)', *Invent. Math.* 178 (2009) 485–504.
15. C. Khare and J.-P. Wintenberger, 'Serre's modularity conjecture (II)', *Invent. Math.* 178 (2009) 505–586.
16. M. Kisin, 'Modularity of 2-adic Barsotti–Tate representations', *Invent. Math.* 178 (2009) 587–634.
17. A. Kraus, 'Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive', *Manuscripta Math.* 69 (1990) 3–385.
18. B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Mat. Inst. Hautes Études Sci.* 47 (1977) 33–186.
19. J. Milne, 'On the arithmetic of abelian varieties', *Invent. Math.* 17 (1972) 177–190.
20. T. Miyake, *Modular forms* (Springer, Berlin, 1989).
21. J. Quer, '$\mathbb{Q}$-curves and abelian varieties of GL_2-type', *Proc. Lond. Math. Soc.* 81 (2000) 285–317.
22. K. Ribet, 'Galois representations attached to eigenforms with nebentypus', *Modular functions of one variable V (Bonn, Germany, 1976)*, Lecture Notes in Mathematics 601 (Springer, Berlin, 1977) 17–51.
23. K. Ribet, 'Report on mod ℓ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$', *Motives (Seattle, WA, 1991)*, Proceedings of Symposia in Pure Mathematics 55 (American Mathematical Society, Providence, RI, 1994) 639–676.
24. J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* 15 (1972) 259–331.
25. J.-P. Serre, 'Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$', *Duke Math. J.* 54 (1987) 179–230.
26. G. Shimura, 'On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields', *Nagoya Math. J.* 43 (1971) 199–208.
27. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).

Imin Chen
Department of Mathematics
Simon Fraser University
Burnaby, British Columbia
V5A 1S6 Canada

ichen@math.sfu.ca

https://doi.org/10.1112/S146115701200006X Published online by Cambridge University Press