Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$

Michael A. Bennett and Imin Chen
Multi-Frey \( \mathbb{Q} \)-curves and the Diophantine equation \( a^2 + b^6 = c^n \)

Michael A. Bennett and Imin Chen

We show that the equation \( a^2 + b^6 = c^n \) has no nontrivial positive integer solutions with \( (a, b) = 1 \) via a combination of techniques based upon the modularity of Galois representations attached to certain \( \mathbb{Q} \)-curves, corresponding surjectivity results of Ellenberg for these representations, and extensions of multi-Frey curve arguments of Siksek.

1. Introduction

Following the proof of Fermat’s last theorem [Wiles 1995], there has developed an extensive literature on connections between the arithmetic of modular abelian varieties and classical Diophantine problems, much of it devoted to solving generalized Fermat equations of the shape

\[
a^p + b^q = c^r, \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1, \tag{1}
\]

in coprime integers \( a, b, \) and \( c, \) and positive integers \( p, q, \) and \( r. \) That the number of such solutions \( (a, b, c) \) is finite, for a fixed triple \( (p, q, r) \), is a consequence of [Darmon and Granville 1995]. It has been conjectured that there are in fact at most finitely many such solutions, even when we allow the triples \( (p, q, r) \) to vary, provided we count solutions corresponding to \( 1^p + 2^3 = 3^2 \) only once. Being extremely optimistic, one might even believe that the known solutions constitute a complete list, namely \( (a, b, c, p, q, r) \) corresponding to \( 1^p + 2^3 = 3^2, \) for \( p \geq 7, \) and to nine other identities (see [Darmon and Granville 1995; Beukers 1998]):

\[
2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2,
17^7 + 76271^3 = 21063928^2, 1414^3 + 2213459^2 = 65^7, 9262^3 + 15312283^2 = 113^7,
43^8 + 96222^3 = 30042907^2, \quad \text{and} \quad 33^8 + 1549034^2 = 15613^3.
\]

Research supported by NSERC.

MSC2010: primary 11D41; secondary 11D61, 11G05, 14G05.

Keywords: Fermat equations, Galois representations, \( \mathbb{Q} \)-curves, multi-Frey techniques.
(For brevity, we omit listing the solutions which differ only by sign changes and permutation of coordinates: for instance, if $p$ is even, $(-1)^p + 2^3 = 3^2$, etc.)

Since all known solutions have $\min\{p, q, r\} < 3$, a closely related formulation is that there are no nontrivial solutions in coprime integers once $\min\{p, q, r\} \geq 3$.

There are a variety of names associated to the above conjectures, including, alphabetically, Beal (see [Mauldin 1997]), Darmon and Granville [1995], van der Poorten, Tijdeman, and Zagier (see, for example, [Beukers 1998; Tijdeman 1989]), and apparently financial rewards have even been offered for their resolution, positive or negative.

Techniques based upon the modularity of Galois representations associated to putative solutions of (1) have, in many cases, provided a fruitful approach to these problems, though the limitations of such methods are still unclear. Each situation where finiteness results have been established for infinite families of triples $(p, q, r)$ has followed along these lines. We summarize the results to date; in each case, no solutions outside those mentioned above have been discovered:

<table>
<thead>
<tr>
<th>$(p, q, r)$</th>
<th>Reference(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(n, n, n), n \geq 3$</td>
<td>[Wiles 1995; Taylor and Wiles 1995]</td>
</tr>
<tr>
<td>$(n, n, 2), n \geq 4$</td>
<td>[Darmon and Merel 1997; Poonen 1998]</td>
</tr>
<tr>
<td>$(n, n, 3), n \geq 3$</td>
<td>[Darmon and Merel 1997; Poonen 1998]</td>
</tr>
<tr>
<td>$(2n, 2n, 5), n \geq 2$</td>
<td>[Bennett 2006]</td>
</tr>
<tr>
<td>$(2, 4, n), n \geq 4$</td>
<td>[Bruin 1999; Ellenberg 2004; Bennett et al. 2010]</td>
</tr>
<tr>
<td>$(2, n, 4), n \geq 4$</td>
<td>Immediate from [Bruin 2003; Bennett and Skinner 2004]</td>
</tr>
<tr>
<td>$(2, 2n, k), n \geq 2, k \in {9, 10, 15}$</td>
<td>[Bennett et al. ≥ 2012]</td>
</tr>
<tr>
<td>$(4, 2n, 3), n \geq 2$</td>
<td>[Bennett et al. ≥ 2012]</td>
</tr>
<tr>
<td>$(2, n, 6), n \geq 3$</td>
<td>[Bennett et al. ≥ 2012]</td>
</tr>
<tr>
<td>$(3, 3, n), n \geq 3^*$</td>
<td>[Kraus 1998; Bruin 2000; Dahmen 2008; Chen and Siksek 2009]</td>
</tr>
<tr>
<td>$(3j, 3k, n), j, k, n \geq 2$</td>
<td>[Kraus 1998]</td>
</tr>
<tr>
<td>$(3, 3, 2n), n \geq 2$</td>
<td>[Bennett et al. ≥ 2012]</td>
</tr>
<tr>
<td>$(3, 6, n), n \geq 2$</td>
<td>[Bennett et al. ≥ 2012]</td>
</tr>
<tr>
<td>$(2, 2n, 3), n \geq 3^*$</td>
<td>[Bruin 1999; Chen 2008; Dahmen 2008; 2011; Siksek 2008]</td>
</tr>
<tr>
<td>$(2, 2n, 5), n \geq 3^*$</td>
<td>[Chen 2010]</td>
</tr>
<tr>
<td>$(2, 3, n), 6 \leq n \leq 10$</td>
<td>[Bruin 1999; 2003; 2005; Poonen et al. 2007; Siksek 2010; Brown 2012]</td>
</tr>
</tbody>
</table>

The $(^*)$ here indicates that the result has been proven for a family of exponents of natural density one (but that there remain infinitely many cases of positive Dirichlet density untreated).
In this paper, we will prove the following theorem.

**Theorem 1.** Let \( n \geq 3 \) be an integer. Then the equation

\[
a^2 + b^6 = c^n
\]

has no solutions in positive integers \( a, b, \) and \( c, \) with \( a \) and \( b \) coprime.

Our motivations for considering this problem are two-fold. Firstly, the exponents \((2, 6, n)\) provide one of the final examples of an exponent family for which there is known to exist a corresponding family of Frey–Hellegouarch elliptic \( \mathbb{Q} \)-curves. A remarkable program for attacking the generalized Fermat equation of signature \((n, n, m)\) (and perhaps others) is outlined in [Darmon 2000], relying upon the construction of Frey–Hellegouarch abelian varieties. Currently, however, it does not appear that the corresponding technology is suitably advanced to allow the application of such arguments to completely solve families of such equations for fixed \( m \geq 5 \).

In some sense, the signatures \((2, 6, n)\) and \((2, n, 6)\) (the latter equations are treated in [Bennett et al. \( \geq 2012 \)]) represent the final remaining families of generalized Fermat equations approachable by current techniques. More specifically, as discussed in [Darmon and Granville 1995], associated to a generalized Fermat equation \( x^p + y^q = z^r \) is a triangle Fuchsian group with signature \((1/p, 1/q, 1/r)\). A reasonable precondition to applying the modular method using rational elliptic curves or \( \mathbb{Q} \)-curves is that this triangle group be commensurable with the full modular group. Such a classification has been performed in [Takeuchi 1977], where it is shown that the possible signatures containing \( \infty \) are \((2, 3, \infty), (2, 4, \infty), (2, 6, \infty), (2, \infty, \infty), (3, 3, \infty), (3, \infty, \infty), (4, 4, \infty), (6, 6, \infty), (\infty, \infty, \infty)\). A related classification of Frey representations for prime exponents can be found in [Darmon and Granville 1995; Darmon 2000]. The above list does not, admittedly, explain all the possible families of generalized Fermat equations that have been amenable to the modular method. In all other known cases, however, the Frey curve utilized is derived from a descent step to one of the above “pure” Frey curve families. Concerning the applicability of using certain families of \( \mathbb{Q} \)-curves, see the conclusions section of [Chen 2010] for further remarks.

Our secondary motivation is as an illustration of the utility of the multi-Frey techniques of S. Siksek (see [Bugeaud et al. 2008a; 2008b]). A fundamental difference between the case of signature \((2, 4, n)\) considered in [Ellenberg 2004] and that of \((2, 6, n)\) is the existence, in this latter situation, of a potential obstruction to our arguments in the guise of a particular modular form *without* complex multiplication. To eliminate the possibility of a solution to the equation \( x^2 + y^6 = z^n \) arising from this form requires fundamentally new techniques, based upon a generalization of the multi-Frey technique to \( \mathbb{Q} \)-curves (rather than just curves over \( \mathbb{Q} \)).
The computations in this paper were performed in MAGMA [Bosma et al. 1997]. The programs, data, and output files are posted in this paper’s Electronic Supplement and at http://people.math.sfu.ca/ichen/firstb3i-data. Throughout the text, we have included specific references to the MAGMA code employed, indicated as sample.txt.

2. Review of $\mathbb{Q}$-curves and their attached Galois representations

The exposition of $\mathbb{Q}$-curves and their attached Galois representations we provide in this section closely follows that of [Ribet 1992; Quer 2000; Ellenberg and Skinner 2001; Chen 2012]; we include it in the interest of keeping our exposition reasonably self-contained.

Let $K$ be a number field and $C/K$ be a non-CM elliptic curve such that there is an isogeny $\mu(\sigma) : C \to C$ defined over $K$ for each $\sigma \in G_Q$. Such a curve $C/K$ is called a $\mathbb{Q}$-curve defined over $K$. Let $\hat{\phi}_{C,p} : G_K \to GL_2(\mathbb{Z}_p)$ be the representation of $G_K$ on the Tate module $\hat{V}_p(C)$. One can attach a representation $\hat{\rho}_{C,\beta,p} : G_Q \to \mathbb{Q}_p^* GL_2(\mathbb{Q}_p)$ to $C$ such that $[\rho_{C,\beta,p}]_{G_K} \cong \hat{\phi}_{C,p}$. The representation depends on the choice of splitting map $\beta$ (in what follows, we will provide more details of this choice). Let $\pi$ be a prime above $p$ of the field $M_\beta$ generated by the values of $\beta$. In practice, the representation $\hat{\rho}_{C,\beta,\pi}$ is constructed in a way so that its image lies in $M_\beta^* GL_2(\mathbb{Q}_p)$, and we choose to use the notation $\hat{\rho}_{C,\beta,p} = \hat{\rho}_{C,\beta,\pi}$ to indicate the choice of $\pi$ in this explicit construction.

Let

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

where $\mu_C^{-1} := (1/\deg \mu_C)\mu_C'$ and $\mu_C'$ is the dual of $\mu_C$. Then $c_C(\sigma, \tau)$ determines a class in $H^2(G_Q, \mathbb{Q}^*)$ which depends only on the $\mathbb{Q}$-isogeny class of $C$. The class $c_C(\sigma, \tau)$ factors through $H^2(G_{K/Q}, \mathbb{Q}^*)$, depending now 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 $\alpha \in H^1(G_Q, \mathbb{Q}^*/\mathbb{Q}^*)$ through the map

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

resulting from the short exact sequence

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

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

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

as cocycles, and we call $\beta$ a splitting map for $c_C$. We define

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

Given a splitting $c_C(\sigma, \tau) = \beta(\sigma) \beta(\tau) \beta(\sigma \tau)^{-1}$, Ribet attaches an abelian variety $A_{\beta}$ defined over $\mathbb{Q}$, of GL$^2$-type and having $C$ as a simple factor over $\mathbb{Q}$.

In practice, what we do in this paper is find a continuous $\beta : G_{\mathbb{Q}} \to \mathbb{Q}^*$, factoring over an extension of low degree, such that $c_C(\sigma, \tau) = \beta(\sigma) \beta(\tau) \beta(\sigma \tau)^{-1}$ as elements in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$, using results in [Quer 2000]. Then we choose a suitable twist $C_{\beta}/K_{\beta}$ of $C$, where $K_{\beta}$ is the splitting field of $\beta$, 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 $A_{\beta}$ is constructed as a quotient over $\mathbb{Q}$ of $\text{Res}_{K_{\beta}/\mathbb{Q}} C_{\beta}$.

The endomorphism algebra of $A_{\beta}$ is given by $M_{\beta} = \mathbb{Q}(\{\beta(\sigma)\}$ and the representation on the $\pi^n$-torsion points of $A_{\beta}$ coincides with the representation $\hat{\rho}_{C, \beta, \pi}$ defined earlier.

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

$$\epsilon(\sigma) = \beta(\sigma)^2 / \deg \mu(\sigma).$$

Then $\epsilon$ is a character and

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

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

3. $\mathbb{Q}$-curves attached to $a^2 + b^6 = c^p$ and their Galois representations

Let $(a, b, c) \in \mathbb{Z}^3$ be a solution to $a^2 + b^6 = c^p$ where we suppose that $p$ is a prime. We call $(a, b, c)$ proper if $\gcd(a, b, c) = 1$ and trivial if $|c| = 1$. Note that a solution $(a, b, c) \in \mathbb{Z}^3$ is proper if and only if the integers $a$, $b$, and $c$ are pairwise coprime. In what follows, we will always assume that the triple $(a, b, c)$ is a proper, nontrivial solution. We consider the following associated (Frey or Frey–Hellegouarch) elliptic curve:

$$E : Y^2 = X^3 - 3(5b^3 + 4ai)bX + 2(11b^6 + 14ib^3a - 2a^2),$$

with $j$-invariant

$$j = 432i \cdot \frac{b^3(4a - 5ib^3)^3}{(a - ib^3)(a + ib^3)^3}$$

and discriminant $\Delta = -2^8 \cdot 3^3 \cdot (a - ib^3) \cdot (a + ib^3)^3$. 


Lemma 2. 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 $j = 54000$, or
- $a/b^3 = \infty$ and $j = 0$.

Proof. This can be seen by solving the polynomial equation in $\mathbb{Q}[i][j, a/b^3]$ derived from (5) by clearing the denominators and collecting terms with respect to $\{1, i\}$, using the restriction that $j, a/b^3 \in \mathbb{P}^1(\mathbb{Q})$.

Corollary 3. $E$ does not have complex multiplication unless

- $a/b^3 = 0$, $j = 54000$, and $d(\mathcal{O}) = -12$, or
- $a/b^3 = \infty$, $j = 0$, and $d(\mathcal{O}) = -3$.

Proof. If $E$ has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field, then $j(E)$ has a real conjugate over $\mathbb{Q}$ (for instance, arising from $j(E_0)$, where $E_0$ is the elliptic curve associated to the lattice $\mathcal{O}$ itself). Hence, $j(E) \in \mathbb{Q}$ in fact. For a list of the $j$-invariants of elliptic curves with complex multiplication by an order of class number 1, see, for instance, [Cox 1989, p. 261].

Lemma 4. If $(a, b, c) \in \mathbb{Z}^3$ with gcd$(a, b, c) = 1$ and $a^2 + b^6 = c^p$, then either $c = 1$ or $c$ is divisible by a prime not equal to 2 or 3.

Proof. The condition gcd$(a, b, c) = 1$ together with inspection of $a^2 + b^6 \pmod{3}$ shows that $c$ is never divisible by 3. Similar reasoning allows us to conclude, since $p > 1$, that $c$ is necessarily odd, whereby the lemma follows.

From here on, let us suppose that $E$ arises from a nontrivial proper solution to $a^2 + b^6 = c^p$ where $p$ is an odd prime. Note that $ab$ is even and, from the preceding discussion, that $a - b^3i$ and $a + b^3i$ are coprime $p$-th powers in $\mathbb{Z}[i]$.

The elliptic curve $E$ is defined over $\mathbb{Q}(i)$. Its conjugate over $\mathbb{Q}(i)$ is $3$-isogenous to $E$ over $\mathbb{Q}(\sqrt{3}, i)$; see [isogeny.txt]. This is in contrast to the situation in [Ellenberg 2004], where the corresponding isogeny is defined over $\mathbb{Q}(i)$. We make a choice of isogenies $\mu(\sigma) : \sigma E \to E$ such that $\mu(\sigma) = 1$ for $\sigma \in G_{\mathbb{Q}(i)}$ and $\mu(\sigma)$ is the $3$-isogeny above when $\sigma \notin G_{\mathbb{Q}(i)}$.

Let $d(\sigma)$ denote the degree of $\mu(\sigma)$. We have $d(G_{\mathbb{Q}}) = \{1, 3\} \subseteq \mathbb{Q}^*/\mathbb{Q}^{*2}$. The fixed field $K_d$ of the kernel of $d(\sigma)$ is $\mathbb{Q}(i)$ and so $(a, d) = (-1, 3)$ is a dual basis in the terminology of [Quer 2000]. The quaternion algebra $(-1, 3)$ is ramified at 2, 3 and so a choice of splitting character for $c_E(\sigma, \tau)$ is given by $\epsilon = \epsilon_2\epsilon_3$ where $\epsilon_2$ is the nontrivial character of $\mathbb{Z}/4\mathbb{Z}^\times$ and $\epsilon_3$ is the nontrivial character of $\mathbb{Z}/3\mathbb{Z}^\times$. The fixed field of $\epsilon$ is $K_{\epsilon} = \mathbb{Q}(\sqrt{3})$.

Let $G_{\mathbb{Q}(i)/\mathbb{Q}} = \{\sigma_1, \sigma_{-1}\}$. We have that

$$\alpha(\sigma_1) = 1 \quad \text{and} \quad \alpha(\sigma_{-1}) = i\sqrt{3}.$$
This can be checked by noting that the quotient of $E$ by the 3-torsion point of $E$ using Vélu multiplies the invariant differential by 1. The resulting quotient elliptic curve is then a twist over $\mathbb{Q} (\sqrt{3}, i)$ of the original $E$. This twisting multiplies the invariant differential by $i \sqrt{3}$.

So now we can express $c_E(\sigma, \tau) = \alpha(\sigma)^{\sigma} \alpha(\sigma) \alpha(\sigma \tau)^{-1}$. Let $\beta(\sigma) = \sqrt{e(\sigma) \sqrt{d(\sigma)}}$ and $c_\beta(\sigma, \tau) = \beta(\sigma) \beta(\tau) \beta(\sigma \tau)^{-1} \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$. We know from [Quer 2000] 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 $\beta$ is $K_\beta = K_\epsilon : K_d = \mathbb{Q} (\sqrt{3}, i)$ and $M_\beta = \mathbb{Q} (\sqrt{3}, i)$.

Our goal is to find a $\gamma \in \mathbb{Q}^*$ such that $c_\beta(\sigma, \tau) = \alpha_1(\sigma)^{\gamma} \alpha_1(\tau) \alpha_1(\sigma \tau)^{-1}$, where $\alpha_1(\sigma) = \alpha(\sigma)^{(\sqrt{3})/\sqrt{3}}$. Using a similar technique as for the equation $a^2 + b^2 = \gamma$ (compare [Chen 2010], where the corresponding $K_\beta$ is cyclic quartic), we can narrow down the possibilities for choices of $\gamma$ and subsequently verify that a particular choice actually works.

In more detail, recall that $K_\beta = \mathbb{Q} (\sqrt{3}, i) = \mathbb{Q} (z)$, where $z = (i + \sqrt{3})/2$ is a primitive twelfth root of unity. Let $G_{\mathbb{Q} (\sqrt{3}, i)/\mathbb{Q}} = \{1, \sigma_1, \ldots, \sigma_3, \sigma_3, \sigma_3, \sigma_3\}$ and assume that $\alpha_1(\sigma_3)^2 / (\sigma_3) - 3$ is a unit, say 1. This implies that $\sigma^{-1} \gamma / \gamma = 1$, whereby $\gamma \in \mathbb{Q} (\sqrt{3})$. Furthermore, let us assume that $\sigma^{-1} \gamma / \gamma$ is a square in $K_\beta$ of a unit in $\mathbb{Q} (\sqrt{3})$, say $z^2$ (the other choices produce isomorphic twists). Solving for $\gamma$, we obtain that $\gamma = (-3 + i \sqrt{3})/2$ is one possible choice.

The resulting values of $\alpha_2(\sigma) = \alpha(\sigma)^{(\sqrt{3})/\sqrt{3}}$ are

$$\alpha_2(\sigma_1) = 1, \quad \alpha_2(\sigma_{-1}) = i \sqrt{3} z, \quad \alpha_2(\sigma_3) = z, \quad \text{and} \quad \alpha_2(\sigma_{-3}) = i \sqrt{3},$$

where we have fixed a choice of square root for each $\sigma \in G_{K/\mathbb{Q}}$. It can be verified that $c_\beta(\sigma, \tau) = \alpha_2(\sigma)^{\gamma} \alpha_2(\tau) \alpha_2(\sigma \tau)^{-1}$.

Consider the twist $E_\beta$ of $E$ given by the equation

$$E_\beta : Y^2 = X^3 - 3(5b^3 + 4ai) b \gamma^2 X + 2(11b_6 + 14ib_3 a - 2a^2) \gamma^3.$$

(6)

From the relationship between $E_\beta$ and $E$, the initial $\mu(\sigma)$’s for $E$ give rise to choices for $\mu_\beta(\sigma)$ for $E_\beta$ which are, in general, locally constant on a smaller subgroup than $G_K$. For these choices of $\mu_\beta(\sigma)$ we have

$$\alpha_{E_\beta}(\sigma) = \alpha_1(\sigma) = \alpha(\sigma)^{(\sqrt{3})/\sqrt{3}}.$$

Now, $\sqrt{(\sqrt{3})/\sqrt{3}} = \xi(\sigma) \delta(\sigma)$ where $\delta(\sigma) = \alpha(\sigma)^{(\sqrt{3})/\sqrt{3}}$ and $\xi(\sigma) = \pm 1$. Since $\delta(\sigma)^{\gamma} \delta(\tau) \delta(\sigma \tau)^{-1} = 1$, it follows that $c_{E_{\beta}}(\sigma, \tau) = c_\beta(\sigma, \tau) \xi(\sigma) \xi(\tau) \xi(\sigma \tau)^{-1}$. Hence, by using the alternate set of isogenies $\mu_\beta(\sigma) = \mu_\beta(\sigma) \xi(\sigma)$, which are now locally constant on $G_K$, the corresponding $a_{E_\beta}(\sigma) = \alpha(\sigma)^{(\sqrt{3})/\sqrt{3}} = \alpha_2(\sigma)$, and hence $c_{E_\beta}(\sigma, \tau) = \alpha_2(\sigma) \alpha_2(\tau) \alpha_2(\sigma \tau)^{-1} = c_\beta(\sigma, \tau)$ as cocycles, not just as classes in $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$. The elliptic curve $E_\beta/K_\beta$ is a $\mathbb{Q}$-curve defined over $K_\beta$; see [isogenyp.txt].
Another way to motivate the preceding calculation is as follows. Without loss of generality, we may assume that $\gamma$ is square-free in the ring of integers of $K_\beta$ (if $\gamma$ is a square, then the corresponding $E_\beta$ is isomorphic over $K_\beta$ to $E$). The field $K_\beta$ has class number 1. If $\gamma = \lambda \gamma'$ where $\lambda \in \mathbb{Z}$, then using $\gamma'$ instead of $\gamma$ yields an $E_\beta$ whose $c_{E_\beta}(\sigma, \tau)$ is the same cocycle in $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$. The condition that $\sqrt{\sigma} \gamma/\gamma$ be a square in $K_\beta$ for all $\sigma \in G_{K/\mathbb{Q}}$ shows that only ramified primes divide $\gamma$ and there are two such primes in $K_\beta = \mathbb{Q}(\sqrt{3}, i)$.

The discriminant of $K_\beta$ is $d_{K_\beta/\mathbb{Q}} = 2^4 \cdot 3^2 = 144$. The prime factorizations of $(2)$ and $(3)$ in $K_\beta$ are given by

$$(2) = q_2^2 \quad \text{and} \quad (3) = q_3^2.$$ 

Let $v_2$ and $v_3$ be uniformizers at $q_2$ and $q_3$ respectively with associated valuations $v_2$ and $v_3$. Thus, up to squares, $\gamma$ is a product of a subset of the elements $\{z, u_2, v_2, v_3\}$.

The authors have subsequently learned that a similar technique for finding $\gamma$ also appeared in [Dieulefait and Urroz 2009] (where $K_\beta$ is polyquadratic).

It would be interesting to study the twists $E_\beta$ which arise from other choices of splitting maps. We will not undertake this here.

**Lemma 5.** Suppose that $E$ and $E'$ are elliptic curves defined by

$$E : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

$$E' : Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6,$$

where the $a_i$ and $a'_i$ lie in a discrete valuation ring $\mathfrak{O}$ with uniformizer $v$.

(a) Suppose the valuation at $v$ of the discriminants is, in each case, equal to 12. If $E$ has reduction type $II^*$ and $a'_i \equiv a_i \pmod{v^6}$, then $E'$ also has reduction type $II^*$. If $E$ has reduction type $I_0$ and $a'_i \equiv a_i \pmod{v^6}$, then $E'$ also has reduction type $I_0$.

(b) Suppose the valuation at $v$ of the discriminants is, in each case, equal to 16. If $E$ has reduction type $II$ and $a'_i \equiv a_i \pmod{v^8}$, then $E'$ also has reduction type $II$.

(c) Suppose the Weierstrass equation of $E$ is in minimal form, and $E$ has reduction type $II$ or $III$. If $a'_i \equiv a_i \pmod{v^8}$, then $E'$ has the same reduction type as $E$ and is also in minimal form.

**Proof.** We give a proof for case (a); the remaining cases are similar. Since the discriminants of $E$ and $E'$ have valuation 12, when $E$ and $E'$ are processed through Tate’s algorithm [Silverman 1994], 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 $\text{II}^\ast$, the algorithm applied to $E$ terminates at Step 10. Since the transformations used in Steps 1–10 are translations, they preserve the congruence $a_i \equiv a_i' \pmod{\nu}$ as $E$ and $E'$ are processed through the algorithm, and since the conditions to exit at Steps 1–10 are congruence conditions modulo $\nu$ 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 $\text{I}_0$, the algorithm applied to $E$ reaches Step 11 to loop back a second time to terminate at Step 1 (because the valuation of the discriminant of the model for $E$ is equal to 12). Again, since $a_i' \equiv a_i \pmod{\nu}$, it follows that the algorithm applied to $E'$ also reaches Step 11 to loop back a second time and terminate at Step 1 (again because the valuation of the discriminant of the model for $E'$ is equal to 12). \hfill \Box

**Theorem 6.** The conductor of $E_\beta$ is

$$m = q_2^4 \cdot q_3^\varepsilon \prod_{q|c \land q \neq 2, 3} q,$$

where $\varepsilon = 0, 4$.

**Proof.** See [late2m.txt] and [late3m.txt] for the computations. Recall that $E_\beta$ is given by

$$E_\beta : Y^2 = X^3 - 3(5b^3 + 4ai)b\gamma^2 X + 2(11b^6 + 14ib^3 a - 2a^2)\gamma^3,$$

with

$$\Delta_{E_\beta} = -2^8 \cdot 3^3 \cdot (a - ib^3)(a + ib^3)^3 \cdot \gamma^6. \quad (8)$$

Then

$$c_4 = 2^4 \cdot 3^2 \cdot b(4ia + 5b^3) \cdot \gamma^2$$

$$c_6 = 2^5 \cdot 3^3 \cdot (2a + (-7i - 6\varepsilon^2 + 3)b^3)(2a + (-7i + 6\varepsilon^2 - 3)b^3) \cdot \gamma^3. \quad (9)$$

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

$$b^3 \equiv 0 \pmod{q} \quad \text{or} \quad 4ia + 5b^3 \equiv 0 \pmod{q},$$

and

$$2a + (-7i - 6\varepsilon^2 + 3)b^3 \equiv 0 \pmod{q} \quad \text{or} \quad 2a + (-7i + 6\varepsilon^2 - 3)b^3 \equiv 0 \pmod{q}.$$  

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. It follows that $E_\beta$ has bad multiplicative reduction at $q$.  


By (8), since $\gcd(a, b) = 1$, we have $v_3(\Delta_{E_\beta}) = 12$. We run through all possibilities for $(a, b)$ modulo $v_3^8$ and, in each case, we compute the reduction type of $E_\beta$ at $q_3$ using MAGMA; in every case, said reduction type turns out to be of type $II^*$ or $I_0$. By Lemma 5(a), this determines all the possible conductor exponents for $E_\beta$ at $q_3$.

Since $a$ and $b$ are of opposite parity, (8) implies that $v_2(\Delta_{E_\beta}) = 16$. Checking all possibilities for $(a, b)$ modulo $v_2^8$, and in each case computing the reduction type of $E_\beta$ at $q_2$, via MAGMA, we always arrive at reduction type $II$. By Lemma 5(b), this determines all the possible conductor exponents for $E_\beta$ at $q_2$. □

Theorem 7. The conductor of $\text{Res}^K_{Q} E_\beta$ is

$$d_{K_\beta/Q}^2 \cdot N_{K_\beta/Q}(m) = 2^{16} \cdot 3^{4+2\varepsilon} \cdot \prod_{q|c, q \neq 2, 3} q^4,$$

where $\varepsilon = 0, 4$.

Proof. See [Milne 1972, Lemma, p. 178]. We also note that $K_\beta$ is unramified outside $\{2, 3\}$ so the product is of the form stated. □

Corollary 8. The elliptic curve $E_\beta$ has potentially good reduction at $q_2$ and $q_3$. In the latter case, the reduction is potentially supersingular.

Let $A = \text{Res}^K_{Q} E_\beta$. By [Quer 2000, Theorem 5.4], $A$ is an abelian variety of $GL_2$ type with $M_\beta = Q(\sqrt{3}, i)$. The conductor of the system of $M_\beta, \pi[G_Q]$-modules $\{\hat{V}_\pi(A)\}$ is given by

$$2^4 \cdot 3^{1+\varepsilon/2} \cdot \prod_{q|c, q \neq 2, 3} q,$$  \hspace{1cm} (10)

using the conductor results explained in [Chen 2010].

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

Theorem 9. 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 bad multiplicative reduction at primes above $p$ when $p \neq 2, 3$, and in the case of bad multiplicative reduction, the exponent of a prime above $p$ in the minimal discriminant of $E$ is divisible by $p$. Also, $p$ is unramified in $K_\beta$ so that $I_p \subseteq G_{K_\beta}$. □

Theorem 10. 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 bad multiplicative reduction at primes above $\ell$ when $\ell \neq 2, 3$, and, in the case of bad multiplicative reduction, the exponent of a prime above $\ell$ in the minimal discriminant of $E$ is divisible by $p$. Also, $\ell$ is unramified in $K_\beta$ so that $I_\ell \subseteq G_{K_\beta}$. □
Theorem 11. Suppose $p \neq 2, 3$. The conductor of $\rho = \rho_{E, \beta, \pi}$ is one of 48 or 432.

Proof. Since we are determining the Artin conductor of $\rho$, we consider only ramification at primes above $\ell \neq p$.

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

Suppose $\ell = 2, 3$. The representation $\hat{\rho}_{E,p} |_{I_\ell}$ factors through a finite group of order only divisible 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 only divisible by the primes 2 and 3. It follows that the exponent of $\ell$ in the conductor of $\rho$ is the same as in the conductor of $\hat{\rho}$ as $p \neq 2, 3$. \qed

Proposition 12. Suppose $p \neq 2, 3$. Then the weight of $\rho = \rho_{E, \beta, \pi}$ is 2.

Proof. The weight of $\rho$ is determined by $\rho |_{I_p}$. Since $p \neq 2, 3$, we see that $K_\beta$ is unramified at $p$ and hence $G_{K_\beta}$ 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 $p$-th cyclotomic character, the weight of $\rho$ is necessarily 2 [Serre 1987, Proposition 4]. \qed

Proposition 13. The character of $\rho_{E, \beta, \pi}$ is $\epsilon$.

Proof. This follows from (4). \qed

Let $X^K_{0,B}(d, p)$, $X^K_{0,N}(d, p)$, and $X^K_{0,N'}(d, p)$ be the modular curves with level-$p$ structure corresponding to a Borel subgroup $B$, the normalizer of a split Cartan subgroup $N$, the normalizer of a nonsplit Cartan subgroup $N'$ of $GL_2(F_p)$, and level-$d$ structure consisting of a cyclic subgroup of order $d$, twisted by the quadratic character associated to $K$ through the action of the Fricke involution $w_d$.

Lemma 14. Let $E$ be a $\mathbb{Q}$-curve defined over $K'$, $K$ a quadratic number field contained in $K'$, and $d$ a prime number such that

(a) the elliptic curve $E$ is defined over $K$,

(b) the choices of $\mu_E(\sigma)$ are constant on $G_K$ cosets, $\mu_E(\sigma) = 1$ when $\sigma \in G_K$,

and $\deg \mu_E(\sigma) = d$ when $\sigma \notin G_K$, and

(c) $\mu_E(\sigma)^d \mu_E(\sigma) = \pm d$ whenever $\sigma \notin G_K$.

If $\rho_{E, \beta, \pi}$ has image lying in a Borel subgroup, normalizer of a split Cartan subgroup, or normalizer of a nonsplit Cartan subgroup of $\hat{\mathbb{F}}_p \times GL_2(F_p)$, then $E$ gives rise to a $\mathbb{Q}$-rational point on the corresponding modular curve above.

Proof. This proof is based on [Ellenberg 2004, Proposition 2.2]. Recall the action of $G_{\mathbb{Q}}$ on $\hat{\mathbb{P}}_E[d]$ is given by $x \mapsto \mu_E(\sigma)(\langle c \rangle x)$. Suppose $\hat{\mathbb{P}} \rho_{E, \beta, p}$ has image lying in a Borel subgroup. Then we have that $\mu_E(\sigma)(\langle C_p \rangle) = C_p$ for some cyclic subgroup $C_p$ of order $p$ in $E[p]$ and all $\sigma \in G_{\mathbb{Q}}$. Let $C_d$ be the cyclic subgroup of order $d$ in
$E[d]$ defined by $\mu_E(\sigma)(\sigma E[d])$ where $\sigma$ is an element of $G_\mathbb{Q}$ which is nontrivial on $K$. This does not depend on the choice of $\sigma$. Suppose $\sigma$ is an element of $G_\mathbb{Q}$ which is nontrivial on $K$. The kernel of $\mu_E(\sigma)$ is precisely $\sigma C_d$ as $\mu_E(\sigma)(\sigma C_d) = (\mu_E(\sigma)\sigma E(\sigma))(\sigma E[d]) = [\pm d]\sigma E[d] = 0$. Hence, we see that

$$w_d(\sigma E, C_d, C_p) = w_d(\sigma E, \sigma C_d, \sigma C_p)$$

$$= (\mu_E(\sigma)\sigma E, \mu_E(\sigma)(\sigma E[d]), \mu_E(\sigma)(\sigma C_p))$$

$$= (E, C_d, C_p),$$

so $\sigma (E, C_d, C_p) = w_d(E, C_d, C_p)$, where $w_d$ is the Fricke involution. Suppose $\sigma$ is an element of $G_\mathbb{Q}$ which is trivial on $K$. In this case, we have $\sigma (E, C_d, C_p) = (E, C_d, C_p)$. Thus, $(E, C_d, C_p)$ gives rise to a $\mathbb{Q}$-rational point on $X_{0,B}(d, p)$.

The case when the image of $\rho_{E, \beta, \pi}$ lies in the normalizer of a Cartan subgroup is similar except now we have the existence of a set of distinct points $S_p = \{\alpha_p, \beta_p\}$ of $\mathbb{P}E[p] \otimes \mathbb{F}_{p^2}$ such that the action of $\sigma \in G_\mathbb{Q}$ by $x \mapsto \mu_E(\sigma)(\sigma x)$ fixes $S_p$ as a set.

**Theorem 15.** Suppose 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 [Ellenberg 2004, Proposition 3.2]. $E$ gives rise to a $\mathbb{Q}$-rational point on $X_{0,N}(3, p)$ by Lemma 14, even though the isogeny between $E$ and its conjugate is only defined over $\mathbb{Q}(\sqrt{3}, i)$. \(\square\)

**Corollary 16.** The representation $\rho_{E, \beta, \pi}$ is irreducible for $p \neq 2, 3, 5, 7, 13$.

**Proof.** Lemma 4 shows that $E$ must have bad multiplicative reduction at some prime of $K$ above $\ell > 3$. \(\square\)

**Proposition 17.** If $p = 13$, then $\rho_{E, \beta, \pi}$ is irreducible.

**Proof.** By Lemma 14, if $\rho_{E, \beta, \pi}$ were reducible, then $E$ would give rise to a noncuspidal $K$-rational point on $X_0(39) \in \mathbb{Q}(i)$ and a noncuspidal $\mathbb{Q}$-rational point on $X_0(39)/w_3$. We can now use [Kenku 1979] which says that $X_0(39)/w_3$ has four $\mathbb{Q}$-rational points. Two of them are cuspidal. Two of them arise from points in $X_0(39)$ defined over $\mathbb{Q}(\sqrt{-7})$. Hence, no such $E$ can exist, since a $K$-rational point on $X_0(39)$ which is also $\mathbb{Q}(\sqrt{-7})$-rational must be $\mathbb{Q}$-rational (and again by [Kenku 1979], $X_0(39)$ has no noncuspidal $\mathbb{Q}$-rational points). \(\square\)

**Outline of proof of Theorem 1.** Using the modularity of $E$, which now follows from Serre’s conjecture [Serre 1987; Khare and Wintenberger 2009a; 2009b; Kisin 2009] plus the usual level-lowering arguments based on results in [Ribet 1990], we have $\rho_{E, \pi, \beta} \cong \rho_{g, \pi}$, where $g$ is a newform in $S_2(\Gamma_0(M), \epsilon)$ where $M = 48$ or $M = 432$. This holds for $n = p \geq 11$. 

718 Michael A. Bennett and Imin Chen
There is one newform $F_1$ in $S_2(\Gamma_0(48), \epsilon)$ and this has CM by $\mathbb{Q}(-3)$; see \[inner-48.txt\] \[cm-48.txt\]. At level 432, we find three newforms $G_1$, $G_2$, and $G_3$ in $S_2(\Gamma_0(432), \epsilon)$; \[inner-432.txt\]. As it transpires, both $G_1$ and $G_2$ have CM by $\mathbb{Q}(-3)$; \[cm-432.txt\]. The form $G_3$ is harder to eliminate as it does not have complex multiplication and its field of coefficients is $M_\beta = \mathbb{Q}(\sqrt{3}, i)$. Furthermore, the complex conjugate of $G_3$ is a twist of $G_3$ by $\epsilon^{-1}$. In fact, $G_3$ arises from the near solution $1^2 + 1^6 = 2$ (this near solution gives rise to a form at level 432 and it is the unique non-CM form at that level) so it shares many of the same properties $g$ should have as both arise from the same geometric construction. Note, however, that one cannot have $a \equiv b \equiv 1 \pmod{2}$ in the equation $a^2 + b^6 = c^p$ as $p > 1$.

Unfortunately, it is not possible to eliminate the possibility of $g = G_3$ by considering the fields cut out by images of inertia at 2. Using [Kraus 1990, théorème 3] and its proof, it can be checked that these fields are the same regardless of whether or not $a \equiv b \equiv 1 \pmod{2}$.

In the next two sections, we show that in each case $g = G_i$, for $i = 1, 2$ (CM case), and $i = 3$, we are led to a contradiction, if $n = p \geq 11$. Finally, in the last section, we deal with the cases $n = 3, 4, 5, 7$. This suffices to prove the theorem as any integer $n \geq 3$ is either divisible by an odd prime or by 4.

4. Eliminating the CM forms

When $g = G_i$ for $i = 1$ or 2, $g$ has complex multiplication by $\mathbb{Q}(\sqrt{-3})$ so that $\rho_{E, \beta, \pi}$ has image lying in the normalizer of a Cartan subgroup for $p > 3$. However, this leads to a contradiction using the arguments below.

**Proposition 18.** Let $p \geq 7$ be prime and suppose there exists either a $p$-newform in $S_2(\Gamma_0(3p^2))$ with $w_p f = f$, $w_3 f = -f$, or a $p$-newform in $S_2(\Gamma_0(p^2))$ with $w_p f = f$, such that $L(f \otimes \chi_{-4}, 1) \neq 0$, where $\chi_{-4}$ is the Dirichlet character associated to $K = \mathbb{Q}(i)$. Let $E$ be an elliptic curve which gives rise to a noncuspidal $\mathbb{Q}$-rational point on $X_{0,N}^K(3, p)$ or $X_{0,N'}^K(3, p)$. Then $E$ has potentially good reduction at all primes of $K$ above $\ell > 3$.

**Proof.** See [Ellenberg 2004] and comments in [Bennett et al. 2010, Proposition 6] about the applicability to the split case (see also the argument in [Ellenberg 2004, Lemma 3.5] which shows potentially good reduction at a prime of $K$ above $p$ in the split case). \[\square\]

**Proposition 19.** If $p \geq 11$ is prime, then there exists a $p$-newform $f \in S_2(\Gamma_0(p^2))$ with $w_p f = f$ and $L(f \otimes \chi_{-4}, 1) \neq 0$.

**Proof.** For $p \geq 61$, this is, essentially, the content of the proof of [Bennett et al. 2010, Proposition 7] (the proof applies to $p \equiv 1 \pmod{8}$, not just to $p \not\equiv 1 \pmod{8}$).
as stated). Further, a relatively short Magma computation reveals the same to be true for smaller values of \( p \) with the following forms \( f \) (the number following the level indicates Magma’s ordering of forms; one should note that this numbering is consistent neither with Stein’s modular forms database nor with Cremona’s tables):

\[
\begin{array}{ccc|ccc|ccc}
 p & f & \text{dim } f & p & f & \text{dim } f & p & f & \text{dim } f \\
11 & 121 (1) & 1 & 29 & 841 (1) & 2 & 47 & 2209 (9) & 16 \\
13 & 169 (2) & 3 & 31 & 961 (1) & 2 & 53 & 2809 (1) & 1 \\
17 & 289 (1) & 1 & 37 & 1369 (1) & 1 & 59 & 3481 (1) & 2 \\
19 & 361 (1) & 1 & 41 & 1681 (1) & 2 & & & \\
23 & 529 (7) & 4 & 43 & 1849 (1) & 1 & & & \\
\end{array}
\]

Theorem 20. Suppose the representation \( \rho_{E,\beta,\pi} \) has image lying in the normalizer of a Cartan subgroup for \( p \geq 11 \). Then \( E \) has potentially good reduction at all primes of \( K \) above \( \ell > 3 \).

Proof. We note that \( E \) still gives rise to a \( \mathbb{Q} \)-rational point on \( X_{0,N}^K(3, p) \) or \( X_{0,N'}^K(3, p) \) with \( K = \mathbb{Q}(i) \), even though, as a consequence of Lemma 14, the isogeny between \( E \) and its conjugate is only defined over \( \mathbb{Q}(\sqrt{3}, i) \).

Theorem 21. If \( p \geq 11 \) is prime, the representation \( \rho_{E,\beta,\pi} \) does not have image lying in the normalizer of a Cartan subgroup.

Proof. Lemma 4 immediately implies that \( E \) necessarily has bad multiplicative reduction at a prime of \( K \) lying above some \( \ell > 3 \).

5. Eliminating the newform \( G_3 \)

Recall that \( E = E_{a,b} \) is given by

\[
E : Y^2 = X^3 - 3(5b^3 + 4ai)bX + 2(11b^6 + 14ib^3a - 2a^2).
\]

Let \( E' = E'_{a,b} \) be the elliptic curve

\[
E' : Y^2 = X^3 + 3b^2X + 2a,
\]

which is a Frey–Hellegouarch elliptic curve over \( \mathbb{Q} \) for the equation \( a^2 + (b^2)^3 = c^p \). We will show how to eliminate the case of \( g = G_3 \) using a combination of congruences from the two Frey curves \( E \) and \( E' \). This is an example of the multi-Frey technique [Bugeaud et al. 2008a; 2008b], as applied to the situation when one of the Frey curves is a \( \mathbb{Q} \)-curve. We are grateful to Siksek for suggesting a version of Lemma 24 which allows us to do this.
The discriminant of $E'$ is given by
\[ \Delta' = -2^6 \cdot 3^3 (a^2 + b^6). \]  
(11)

For $a \neq b \pmod{2}$, $v_2(\Delta') = 6$, so $E'$ is in minimal form at 2. Since $a$ and $b$ are not both multiples of 3, we have $v_3(\Delta') = 3$ and so $E'$ is also minimal at 3. If $q$ divides $\Delta'$ and is neither 2 nor 3, then $E'$ has bad multiplicative reduction at $q$.

For each congruence class of $(a, b)$ modulo $2^4$ where $a \neq b \pmod{2}$, we compute the conductor exponent at 2 of $E'$ using MAGMA. The conductor exponent at 2 of each test case was 5 (reduction type III) or 6 (reduction type II): [late2m-3.txt]. By Lemma 5(c), the conductor exponent at 2 of $E'$ is 5 or 6. In a similar way, the conductor exponent at 3 of $E'$ is 2 (reduction type III) or 3 (reduction type II): [late3m-3.txt].

We are now almost in position to apply the modular method to $E'$. We need only show that the representation $\rho_{E',p}$ arising from the $p$-torsion points of $E'$ is irreducible.

**Lemma 22.** If $p \geq 11$ is prime, then $\rho_{E',p}$ is irreducible.

**Proof.** If $p \neq 13$, the result follows essentially from [Mazur 1978] (see [Dahmen 2008, Theorem 22]), provided $j_{E'}$ is not one of

\[ -2^{15}, -11^2, -11 \cdot 13^3, -\frac{17 \cdot 373^3}{2^{17}}, -\frac{17^2 \cdot 101^3}{2}, -2^{15} \cdot 3^3, -7 \cdot 137^3 \cdot 2083^3, \]
\[ -7 \cdot 11^3, -2^{18} \cdot 3^3 \cdot 5^3, -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3, -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3. \]

Since
\[ j_{E'} = \frac{1728b^6}{a^2 + b^6} > 0, \]

we may thus suppose that $p = 13$. In this case, if $\rho_{E',p}$ were reducible, the representation would correspond to a rational point on the curve defined via the equation $j_{13}(t) = j_{E'}$, where $j_{13}(t)$ is the map from the modular curve $X_0(13)$ to $X(1)$, given by

\[ j_{13}(t) = \frac{(t^4 + 7t^3 + 20t^2 + 19t + 1)^3 (t^2 + 5t + 13)}{t} = \frac{(t^6 + 10t^5 + 46t^4 + 108t^3 + 122t^2 + 38t - 1)^2 (t^2 + 6t + 13)}{t} + 1728. \]

Writing $s = a/b^3$, we thus have $1728/(s^2 + 1) = j_{13}(t)$, for some $t \in \mathbb{Q}$, and so

\[ s^2 = \frac{1728 - j_{13}(t)}{j_{13}(t)} = -\frac{(t^6 + 10t^5 + 46t^4 + 108t^3 + 122t^2 + 38t - 1)^2 (t^2 + 6t + 13)}{(t^4 + 7t^3 + 20t^2 + 19t + 1)^3 (t^2 + 5t + 13)}. \]
It follows that there exist rational numbers \( x \) and \( y \) with
\[
y^2 = -(x^2 + 6x + 13)(x^2 + 5x + 13)(x^4 + 7x^3 + 20x^2 + 19x + 1),
\]
and hence coprime, nonzero integers \( u \) and \( v \), and an integer \( z \) for which
\[
(u^2 + 6uv + 13v^2)(u^2 + 5uv + 13v^2)(u^4 + 7u^3v + 20u^2v^2 + 19uv^3 + v^4) = -z^2.
\]
Note that, via a routine resultant calculation, if a prime \( p \) divides both \( u^2 + 6uv + 13v^2 \) and the term \((u^2 + 5uv + 13v^2)(u^4 + 7u^3v + 20u^2v^2 + 19uv^3 + v^4)\), then necessarily \( p \in \{2, 3, 13\} \). Since \( u^2 + 6uv + 13v^2 \) is positive-definite and \( u \), and \( v \) are coprime (whereby \( u^2 + 6uv + 13v^2 \equiv \pm 1 \pmod{3} \)), we thus have
\[
(u^2 + 6uv + 13v^2) = 2^{b_1}13^{b_2}z_1^2,
\]
\[
(u^2 + 5uv + 13v^2)(u^4 + 7u^3v + 20u^2v^2 + 19uv^3 + v^4) = -2^{b_1}13^{b_2}z_2^2,
\]
for \( z_1, z_2 \in \mathbb{Z} \) and \( \delta_i \in \{0, 1\} \). The first equation, with \( \delta_1 = 1 \), implies that \( u \equiv v \equiv 1 \pmod{2} \), contradicting the second. We thus have \( \delta_1 = 0 \), whence
\[
u^2 + 6uv + 13v^2 \equiv u^2 + v^2 \equiv z_1^2 \equiv 1 \pmod{3},
\]
so that 3 divides one of \( u \) and \( v \), again contradicting the second equation, this time modulo 3. \( \square \)

Applying the modular method with \( E' \) as the Frey curve thus shows that \( \rho_{E', p} \cong \rho_{g', \pi'} \) for some newform \( g' \in S_2(\Gamma_0(M)) \) where \( M = 2^r 3^s \), \( r \in \{5, 6\} \), and \( s \in \{2, 3\} \) (here \( \pi' \) is a prime above \( p \) in the field of coefficients of \( g' \)). The possible forms \( g' \) were computed using \texttt{b3i-modformagain.txt}. The reason the multi-Frey method works is because when \( a \not\equiv b \pmod{2} \), we that \( r \in \{5, 6\} \), whereas when \( a \equiv b \equiv 1 \pmod{2} \), we have \( r = 7 \). Thus, the 2-part of the conductor of \( \rho_{E', \pi} \) separates the cases \( a \not\equiv b \pmod{2} \) and \( a \equiv b \pmod{2} \). Hence, the newform \( g' \) that the near solution \( a = b = 1 \) produces does not cause trouble 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 \( E \), by appealing to the multi-Frey technique.

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

**Lemma 23.** Let \( q \geq 5 \) be prime and assume \( q \neq p \), where \( p \geq 11 \) is a prime. Let
\[
C_{x, y}(q, g') = \begin{cases} a_q(E'_x, y) - a_q(g') & \text{if } x^2 + y^6 \not\equiv 0 \pmod{q}, \\ (q + 1)^2 - a_q(g')^2 & \text{if } x^2 + y^6 \equiv 0 \pmod{q}. \end{cases}
\]
If \( (a, b) \equiv (x, y) \pmod{q} \), then \( p | C_{x, y}(q, g') \).
We wish to eliminate the case of Lemma 24. Let \( q \) be prime and assume \( q \not\equiv 1 \pmod{p} \), where \( p \) is prime. The following is the analog of Lemma 23 for \( E = E_{a,b} \).

**Lemma 24.** Let \( q \geq 5 \) be prime and assume \( q \not\equiv 1 \pmod{p} \), where \( p \geq 11 \) is prime. Let

\[
B_{x,y}(q, g) = \begin{cases} 
N(a_q(E_{x,y})^2 - \epsilon(q)a_q(g)^2) & \text{if } x^2 + y^6 \not\equiv 0 \pmod{q} \text{ and } \left(\frac{-4}{q}\right) = 1, \\
N(a_q(g)^2 - a_q(E_{x,y} - 2q\epsilon(q))) & \text{if } x^2 + y^6 \not\equiv 0 \pmod{q} \text{ and } \left(\frac{-4}{q}\right) = -1, \\
N(\epsilon(q)(q+1)^2 - a_q(g)^2) & \text{if } x^2 + y^6 \equiv 0 \pmod{q},
\end{cases}
\]

where \( a_q(E_{x,y}) \) is the trace of \( \text{Frob}_q^i \) acting on the Tate module \( T_p(E_{x,y}) \).

If \((a, b) \equiv (x, y) \pmod{q}\), then \( p | B_{x,y}(q, g) \).

**Proof.** Recall the setup in Sections 2 and 3. Let \( \pi \) be a prime of \( M_\beta \) above \( p \). The mod \( \pi \) representation \( \rho_{A_\beta, \pi} \) of \( G_K \) attached to \( A_\beta \) is related to \( E_\beta \) 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 \( E_\beta \), and the \( \mathbb{P} \) indicates that we are considering isomorphism up to scalars. The algebraic formula which describes \( \rho_{E_\beta, \pi} = \rho_{A_\beta, \pi} \cong \rho_{f, \pi} \) 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 \( ^aE_\beta \to E_\beta \) for each \( \sigma \) which is constant on \( G_K \) (see the paragraph after (6)).

If \( x^2 + y^6 \equiv 0 \pmod{q} \), then \( q | c \). Recall the conductor of \( A_\beta \) is given by

\[
2^4 \cdot 3^{1+\epsilon/2} \cdot \prod_{q \mid c, q \neq 2,3} q,
\]

so that \( q \) exactly divides the conductor of \( A_\beta \). Using the condition \( \rho_{f, \pi} \cong \rho_{g, \pi} \), we can deduce from [Carayol 1983, théorème 2.1], [Carayol 1986, théorème (A)], [Darmon et al. 1997, Theorem 3.1], and [Gross 1990, (0.1)] that

\[
p | N(a_q(g)^2 - \epsilon^{-1}(q)(q+1)^2).
\]

If \( x^2 + y^6 \not\equiv 0 \pmod{q} \), then let \( q \) be a prime of \( K_\beta \) over \( q \). Let \( \overline{E} = \overline{E}_{a,b} \) be the reduction modulo \( q \) of \( E \). Since \((a, b) \equiv (x, y) \pmod{q} \), we have \( \overline{E} = E_{x,y} \).

Furthermore, since \( q \) is a prime of good reduction, \( T_p(E) \cong T_p(\overline{E}) \).
We now wish to relate the representation $\rho_{E,\beta,\pi} = \rho_{A,\beta,\pi} \cong \rho_{f,\pi}$ to the representation $\phi_{E,p}$ for the original $E$. We know that

$$c_{E,\beta}(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma \tau)^{-1} \quad \text{and} \quad c_{E,\beta}(\sigma, \tau) = c_E(\sigma, \tau)\kappa(\sigma)\kappa(\tau)\kappa(\sigma \tau)^{-1},$$

where $\kappa(\sigma) = \frac{\sigma(\sqrt{\gamma})}{\sqrt{\gamma}}$ and $\gamma = \frac{-3 + i\sqrt{3}}{2}$. It follows that

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

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

Now we have

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

where $1 \otimes x \in M_{\beta,\pi} \otimes T_p(E)$. For this choice of $\beta'(\sigma)$,

$$\rho_{A,\beta',\pi} \cong \kappa(\sigma)\xi(\sigma) \otimes \rho_{A,\beta,\pi} \cong \kappa(\sigma)\xi(\sigma) \otimes \rho_{f,\pi}.$$ 

This can be seen by fixing the isomorphism $\iota : E \cong E_\beta$, using standard Weierstrass models and then appealing to the

$$E_\beta \xrightarrow{\sigma} \sigma E_\beta \xrightarrow{\mu_E(\sigma)} \sigma E \xrightarrow{\iota} E,$$

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 $\sigma \in G_{Q(\sqrt{-1})}$ and $d(\sigma) = 3$ if $\sigma \notin G_{Q(\sqrt{-1})}$.

Now $\left(\frac{-4}{q}\right) = 1$ means $\sigma = \text{Frob}_q \in G_{Q(\sqrt{-1})}$. If $\sigma \in G_{Q(\sqrt{-1})}$, then $\mu(\sigma) = \text{id}$ and $d(\sigma) = 1$ so

$$\rho_{A,\beta',\pi}(\sigma)(1 \otimes x) = \beta'(\sigma)^{-1} \otimes \mu(\sigma)(\phi_{E,p}(\sigma)(x)) = \sqrt{\epsilon(\sigma)^{-1}}\kappa(\sigma)^{-1} \otimes \phi_{E,p}(\sigma)(x),$$

so $\text{tr} \rho_{A,\beta,\pi}(\sigma) = \sqrt{\epsilon(\sigma)^{-1}}\kappa(\sigma)^{-1} \cdot \text{tr} \phi_{E,p}(\sigma)$ and $\epsilon(q)a_q(f)^2 = a_q(E)^2$. Also $a_q(f) \equiv a_q(g) \pmod{\pi}$, giving the assertion that $p|B_q(q, g)$ in the case $\left(\frac{-4}{q}\right) = 1$.

If $\left(\frac{-4}{q}\right) = -1$, then $\sigma = \text{Frob}_q \notin G_{Q(\sqrt{-1})}$. But then $\sigma^2 \in G_{Q(\sqrt{-1})}$, and in fact, $\sigma^2 \in G_{Q(\sqrt{-1}, \sqrt{3})}$, so by the argument above we get

$$\text{tr} \rho_{A,\beta,\pi}(\sigma^2) = \sqrt{\epsilon(\sigma)^{-1}}\kappa(\sigma)^{-1} \cdot \text{tr} \phi_{E,p}(\sigma^2) = \text{tr} \phi_{E,p}(\sigma^2) = a_q^2(E).$$
Also, \( tr \rho_{A_{p_0}, \pi}(\sigma) = \kappa(\sigma) \xi(\sigma) a_q(f) \) so \( tr \rho_{A_{p_0}, \pi}(\sigma)^2 = a_q(f)^2 \). We have
\[
\frac{1}{\det(1 - \rho_{A_{p_0}, \pi}(\sigma)q^{-s})} = \exp \sum_{r=1}^{\infty} tr \rho_{A_{p_0}, \pi}(\sigma^r)q^{-sr} = \frac{1}{1 - tr \rho_{A_{p_0}, \pi}(\sigma)q^{-s} + q \epsilon(q)q^{-2s}}.
\]

The determinant and traces are of vector spaces over \( M_{\beta, \pi} \). Computing the coefficient of \( q^{-2s} \) and equating, we find that \( tr \rho_{A_{p_0}, \pi}(\sigma^2) = tr \rho_{A_{p_0}, \pi}(\sigma)^2 - 2q \epsilon(q) \) and hence conclude that \( a_q(f)^2 - 2q \epsilon(q) = a_q(z(E)) \). Since \( a_q(f) \equiv a_q(g) \mod \pi \), it follows that \( p|B_\alpha(q, g) \) in the case \( (\frac{c}{q}) = -1 \) as well.

Let
\[
A_q(g, g') := \prod_{(x, y) \in \mathbb{Z}_q^2} gcd(B_{x, y}(q, g), C_{x, y}(q, g')).
\]

Then we must have \( p|A_q(g, g') \). 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 \( g = G_3 \), and \( g' \) running through the newforms in \( S_2(\Gamma_0(2^r 3^s)) \) where \( r \in \{5, 6\} \) and \( s \in \{2, 3\} \), the above process eliminates all possible pairs \( g = G_3 \) and \( g' \); see \texttt{multi-frey.txt}. In particular, using \( q = 5 \) or \( q = 7 \) for each pair shows that \( p \in \{2, 3, 5\} \). Hence, if \( p \notin \{2, 3, 5, 7\} \), then a solution to our original equation cannot arise from the newform \( g = G_3 \).

6. The cases \( n = 3, 4, 5, 7 \)

It thus remains only to treat the equation \( a^2 + b^6 = c^n \) for \( n \in \{3, 4, 5, 7\} \). In each case, without loss of generality, we may suppose that we have a proper, nontrivial solution in positive integers \( a, b, \) and \( c \). If \( n = 4 \) or \( 7 \), the desired result is immediate from [Bruin 1999] and [Poonen et al. 2007], respectively. In the case \( n = 3 \), a solution with \( b \neq 0 \) implies, via the equation
\[
\left( \frac{a}{b^3} \right)^2 = \left( \frac{c}{b^2} \right)^3 - 1,
\]
a rational point on the elliptic curve given by \( E : y^2 = x^3 - 1 \), Cremona’s 144A1 of rank 0 over \( \mathbb{Q} \) with \( E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \). It follows that \( c = b^2 \) and hence \( a = 0 \).

Finally, we suppose that \( a^2 + b^6 = c^5 \), for coprime positive integers \( a, b, \) and \( c \). From parametrizations for solutions to \( x^2 + y^2 = z^5 \) (see, for example, [Chen 2010, Lemma 2]), it is easy to show that there exist coprime integers \( u \) and \( v \) (and \( z \)) for which
\[
v^4 - 10v^2u^2 + 5u^4 = 5^6z^3,
\]
(12)
with either
(a) \( v = \beta^3, \delta = 0, \beta \) coprime to 5, or
(b) \( v = 5^2 \beta^3, \delta = 1, \) for some integer \( \beta. \)

Let us begin by treating the latter case. From (12), we have
\[
(u^2 - v^2)^2 - 4 \cdot 5^7 \cdot \beta^{12} = z^3;
\]
and hence taking
\[
x = \frac{z}{5^2 \beta^4}, \quad y = \frac{u^2 - v^2}{5^3 \beta^6},
\]
we have a rational point on \( E : y^2 = x^3 + 20, \) Cremona’s 2700E1 of rank 0 and trivial torsion (with no corresponding solutions of interest to our original equation).

We may thus suppose that we are in situation (a), so that
\[
\beta^{12} - 10 \beta^6 u^2 + 5 u^4 = z^3. \quad (13)
\]

Since \( \beta \) and \( u \) are coprime, we may assume that they are of opposite parity (and hence that \( z \) is odd), since \( \beta \equiv u \equiv 1 \pmod{2} \) with (13) leads to an immediate contradiction modulo 8. Writing \( T = \beta^6 - 5 u^2, \) (13) becomes \( T^2 - 20 u^4 = z^3, \) where \( T \) is coprime to 10. Factoring over \( \mathbb{Q}(\sqrt{5}) \) (which has class number 1), we deduce the existence of integers \( m \) and \( n, \) of the same parity, such that
\[
T + 2 \sqrt{5} u^2 = \left( \frac{1 + \sqrt{5}}{2} \right)^\delta \left( \frac{m + n \sqrt{5}}{2} \right)^3, \quad (14)
\]
with \( \delta \in \{0, 1, 2\}. \)

Let us first suppose that \( \delta = 1. \) Then, expanding (14), we have
\[
m^3 + 15 m^2 n + 15 m n^2 + 25 n^3 = 16 T \quad \text{and} \quad m^3 + 3 m^2 n + 15 m n^2 + 5 n^3 = 32 u^2.
\]
It follows that
\[
3 m^2 n + 5 n^3 = 4 T - 8 u^2 \equiv 4 \pmod{8},
\]
contradicting the fact that \( m \) and \( n \) have the same parity. Similarly, if \( \delta = 2, \) we find that
\[
3 m^3 + 15 m^2 n + 45 m n^2 + 25 n^3 = 16 T \quad \text{and} \quad m^3 + 9 m^2 n + 15 m n^2 + 15 n^3 = 32 u^2,
\]
and so
\[
3 m^2 n + 5 n^3 = 24 u^2 - 4 T \equiv 4 \pmod{8},
\]
again a contradiction.

We thus have \( \delta = 0, \) and so
\[
m(m^2 + 15 n^2) = 8 T = 8(\beta^6 - 5 u^2) \quad \text{and} \quad n(3 m^2 + 5 n^2) = 16 u^2. \quad (15)
\]
Combining these equations, we may write

$$16\beta^6 = (m + 5n)(2m^2 + 5mn + 5n^2).$$  \hfill (16)

Returning to the last equation of (15), since gcd\(m, n\) divides 2, we necessarily have \(n = 2^\delta_1 3^\delta_2 r^2\) for some integers \(r\) and \(\delta_i \in \{0, 1\}\). Considering the equation \(n(3m^2 + 5n^2) = 16u^2\) modulo 5 implies that \((\delta_1, \delta_2) = (1, 0)\) or \((0, 1)\). In case \((\delta_1, \delta_2) = (1, 0)\), the two equations in (15), taken together, imply a contradiction modulo 9.

We may thus suppose that \((\delta_1, \delta_2) = (0, 1)\) and, setting \(y = (2\beta/r)^3\) and \(x = 6m/n\) in (16), we find that

$$y^2 = (x + 30)(x^2 + 15x + 90).$$

This elliptic curve is Cremona’s 3600G1, of rank 0 with nontrivial torsion corresponding to \(x = -30\), \(y = 0\).

It follows that there do not exist positive coprime integers \(a, b,\) and \(c\) for which \(a^2 + b^6 = c^n\), which completes the proof of Theorem 1.

**Acknowledgements**

The authors would like to thank Samir Siksek and Sander Dahmen for useful suggestions and correspondence pertaining to this paper, and the anonymous referees for numerous helpful comments.

**References**


[Bruin 1999] N. Bruin, “The Diophantine equations \(x^2 + y^4 = \pm z^6\) and \(x^2 + y^8 = z^3\)”, *Compositio Math.* 118:3 (1999), 305–321. MR 2001d:11035 Zbl 0941.11013


Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$


Communicated by Richard Taylor

Received 2010-10-25 Revised 2011-02-23 Accepted 2011-04-01

bennett@math.ubc.ca  Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, BC V6T 1Z2, Canada

ichen@math.sfu.ca  Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC V5A 1S6, Canada
Spherical varieties and integral representations of $L$-functions
Yiannis Sakellaridis

Nonuniruledness results for spaces of rational curves in hypersurfaces
Roya Beheshti

Degeneracy of triality-symmetric morphisms
Dave Anderson

Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$
Michael A. Bennett and Imin Chen

Detaching embedded points
Dawei Chen and Scott Nollet

Moduli of Galois $p$-covers in mixed characteristics
Dan Abramovich and Matthieu Romagny

Block components of the Lie module for the symmetric group
Roger M. Bryant and Karin Erdmann

Basepoint-free theorems: saturation, $b$-divisors, and canonical bundle formula
Osamu Fujino

Realizing large gaps in cohomology for symmetric group modules
David J. Hemmer