JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Michael A. BENNETT, Philippe MICHAUD-JACOBS et Samir SIKSEK

$\mathbb{Q}$-curves and the Lebesgue–Nagell equation

Tome 35, nº 2 (2023), p. 495-510.

https://doi.org/10.5802/jtnb.1254

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **35** (2023), 495–510

$\mathbb{Q}$-curves and the Lebesgue–Nagell equation

par Michael A. BENNETT, Philippe MICHAUD-JACOBS
et Samir SIKSEK

Résumé. Dans cet article, nous considérons l'équation

$$x^2 - q^{2k+1} = y^n, \qquad q \nmid x, \quad 2 \mid y,$$

pour des entiers x, q, k, y et n, avec $k \geq 0$ et $n \geq 3$. Nous prolongeons le travail des premier et troisième auteurs en trouvant toutes les solutions dans les cas $q = 41$ et $q = 97$. Nous faisons ceci en construisant une $\mathbb{Q}$-courbe de Frey–Hellegouarch définie sur le corps quadratique réel $K = \mathbb{Q}(\sqrt{q})$, et en combinant la méthode modulaire avec des techniques multi-Frey.

Abstract. In this paper, we consider the equation

$$x^2 - q^{2k+1} = y^n, \qquad q \nmid x, \quad 2 \mid y,$$

for integers x, q, k, y and n, with $k \geq 0$ and $n \geq 3$. We extend work of the first and third-named authors by finding all solutions in the cases $q = 41$ and $q = 97$. We do this by constructing a Frey–Hellegouarch $\mathbb{Q}$-curve defined over the real quadratic field $K = \mathbb{Q}(\sqrt{q})$, and using the modular method with multi-Frey techniques.

1. Introduction

The equation

$$x^2 + D = y^n \tag{1.1}$$

is known as the *Lebesgue–Nagell equation*. Here, x and y are coprime integers, $n \geq 3$ and D is an integer whose prime divisors belong to a fixed finite set. The Lebesgue–Nagell equation has a rich history and many cases have been resolved through use of a wide variety of techniques, ranging from primitive divisor arguments and bounds for linear forms in logarithms, to the modular method, based upon the modularity of Galois representations attached to Frey–Hellegouarch curves.

Manuscrit reçu le 18 février 2022, révisé le 5 septembre 2022, accepté le 23 septembre 2022.
2020 *Mathematics Subject Classification.* 11D41, 11D61, 11F80, 11G05.
Mots-clefs. Lebesgue–Nagell, Elliptic curves, Frey curve, multi-Frey, $\mathbb{Q}$-curves, modularity, level-lowering, Galois representations, newforms.
The first-named author is supported by NSERC. The second-named author is supported by an EPSRC studentship and has previously used the name Philippe Michaud-Rodgers. The third-named author is supported by an EPSRC Grant EP/S031537/1 "Moduli of elliptic curves and classical Diophantine problems".

In recent papers of the first- and third-named authors [3] and [4], various tools are developed to tackle equation (1.1) in the two "difficult" cases, where either $D > 0$ and y is even, or where $D < 0$. In particular, [3] focusses upon these situations where, additionally, it is assumed that D has a single prime divisor. For primes $q < 100$, the only unsolved cases of the equation $x^2 \pm q^\alpha = y^n$ (see [3, Theorem 3 and Proposition 13.3]) correspond to

$$x^2 - 2 = y^n, \tag{1.2}$$

$$x^2 - q^{2k+1} = y^n, \quad 2 \nmid y, \tag{1.3}$$

for $q \in \{3, 5, 17, 37, 41, 73, 89\}$, and

$$x^2 - q^{2k+1} = y^n, \quad 2 \mid y, \tag{1.4}$$

for $q \in \{17, 41, 89, 97\}$. Here, k is a nonnegative integer and, in each case, we suppose that $n \geq 3$ and that $\gcd(x, y) = 1$. The fundamental obstruction to resolving equations (1.2) and (1.3), for $q \in \{3, 5, 17, 37\}$, lies in the existence of a solution with $y = \pm 1$, valid for all (odd) exponents n. The analogous obstruction, in case of equation (1.3) with $q \in \{41, 73, 89\}$, or equation (1.4), for $q \in \{17, 41, 89, 97\}$, is slightly more subtle, arising from the fact that $q \pm 8$ is square, in the first case, and from the identities

$$23^2 - 17 = 2^9, \quad 13^2 - 41 = 2^7, \quad 91^2 - 89 = 2^{13} \quad \text{and} \quad 15^2 - 97 = 2^7, \tag{1.5}$$

in the second.

In this paper, we will concentrate on equation (1.4), developing new techniques to handle further values of q via the use of $\mathbb{Q}$-curves and multi-Frey techniques, overcoming some of these obstructions. In particular, we will prove the following.

Theorem 1.1. *Let $q \in \{41, 97\}$. Then the solutions to equation* (1.4) *in integers x, y, k, n, with $x, k \geq 0$, $n \geq 3$ and* $\gcd(x, y) = 1$ *are as follows:*

$$(q, x, y, k, n) = (41, 3, -2, 0, 5),\ (41, 7, 2, 0, 3),\ (41, 13, 2, 0, 7),$$
$$(41, 411, 10, 1, 5),\ (97, 15, 2, 0, 7) \ \textit{and} \ (97, 77, 18, 0, 3).$$

We are unable to provide a similar result for the cases $q = 17$ and $q = 89$, with obstructions to our method arising from the first and third identities in (1.5). We will still consider the cases $q = 17$ and $q = 89$ throughout, and in Section 5 will explain precisely why these solutions prevent us from resolving equation (1.4) for these primes q. Note that Barros [1] claims to resolve equations (1.3) and (1.4) in the case $k = 0$ and $q = 89$; his argument overlooks the obstructing solution corresponding to the third identity on (1.5).

Thanks to [3, Theorems 1, 3 and 5] in the case $q = 97$, we obtain the following corollary to Theorem 1.1.

Corollary 1.2. *All solutions to the equation*

$$x^2 \pm 97^\alpha = y^n, \qquad 97 \nmid x,$$

for integers x, α, y and n with $x, \alpha \geq 1$ and $n \geq 3$ are given by

$$(\pm 15)^2 - 97 = 2^7, \ \ (\pm 77)^2 - 97 = 18^3,$$
$$(\pm 175784)^2 - 97^4 = 3135^3 \quad \textit{and} \quad (\pm 48)^2 + 97 = 7^4.$$

$\mathbb{Q}$-curves have been successfully applied to the problem of solving Diophantine equations in the past; the first such example is due to Ellenberg [7], where he treats the equation

$$x^2 + y^4 = z^n,$$

for suitably large n. We refer to [12] for a clear exposition of the general method and the references therein for more examples of this approach; we highlight [2], since the set-up (once the Frey–Hellegouarch $\mathbb{Q}$-curve has been constructed) is most similar to ours.

We now outline the rest of the paper. In Section 2, we will associate a rational Frey–Hellegouarch curve G to equation (1.4) and recall some results from [3]. In Section 3, we construct a second Frey–Hellegouarch curve E, this time defined over the real quadratic field $\mathbb{Q}(\sqrt{q})$, show that it is a $\mathbb{Q}$-curve, and compute its conductor. Then, in Section 4, we will investigate some further properties of this $\mathbb{Q}$-curve, and in particular prove that its restriction of scalars is an abelian surface of GL_2-type, which will allow us to associate the mod n Galois representation of E to a classical newform of a certain level and character. Finally, in Section 5, we will try and eliminate newforms to reach a contradiction.

The `Magma` [5] files used to carry out the computations in this paper are available at `https://github.com/michaud-jacobs/Q-curves`

Acknowledgements. We would like to thank the anonymous referee for a very careful reading of the paper and many helpful comments. The second-named author would like to thank Damiano Testa for many useful discussions.

2. A Rational Frey–Hellegouarch Curve

Let $q \in \{17, 41, 89, 97\}$ and suppose that (x, k, y, n) is a solution to equation (1.4). We will assume that $x \equiv 1 \pmod 4$ by replacing x by $-x$ if necessary. We will also assume that n is prime with $n \geq 7$, since the cases $n \in \{3, 4, 5\}$ are resolved for all values of q in the range $3 \leq q < 100$ in [3, pp. 6–7, 24]. Following [3, Proposition 14.1], we associate a Frey–Hellegouarch elliptic curve, defined over $\mathbb{Q}$, to this solution:

$$G = G_{x,k,q} \ : \ Y^2 = X^3 + 4xX^2 + 4(x^2 - q^{2k+1})X. \tag{2.1}$$

The conductor of G is given by

$$N_G = q\,\mathrm{Rad}(y),$$

where $\mathrm{Rad}(y)$ is the product of the distinct primes dividing the nonzero integer y. We write $\bar{\rho}_{G,n}$ for the mod n Galois representation of the elliptic curve G. Applying standard level-lowering results, followed by the elimination of some newforms at level $2q$ (recall that y is even), we find that $\bar{\rho}_{G,n} \sim \bar{\rho}_{F,n}$ for $F = F_q$ an elliptic curve of conductor $2q$ given, in Cremona's notation, in Table 2.1 (see [3, Proposition 14.1]). Each curve F in Table 2.1 corresponds to (at least) one solution to equation (1.4). We have

$$\begin{aligned}
(-23)^2 - 17 &= 2^9 \quad \text{and} \quad G_{-23,0,17} \cong F_{17},\\
13^2 - 41 &= 2^7 \quad \text{and} \quad G_{13,0,41} \cong F_{41},\\
(-91)^2 - 89 &= 2^{13} \quad \text{and} \quad G_{-91,0,89} \cong F_{89},\\
(-15)^2 - 97 &= 2^7 \quad \text{and} \quad G_{-15,0,97} \cong F_{97}.
\end{aligned}$$

These isomorphisms of elliptic curves prevent us from using the isomorphisms of mod n Galois representations $\bar{\rho}_{G,n} \sim \bar{\rho}_{F,n}$ to obtain an upper bound on n. We can, in fact, deduce such a bound through appeal to linear forms in logarithms, but it will be impractically large for our purposes, in each case well in excess of 10^{10}. It is worth observing that equation (1.4) is the more problematical case (in comparison to equation (1.3)), for the purposes of application of bounds for linear forms in logarithms. In case of equation (1.3), results of Bugeaud [6] imply that

$$n < 4.5 \cdot 10^6 q^2 \log^2 q,$$

which we can, with care, sharpen to an upper bound upon n of somewhat less than 10^6 for, say, $q = 3$ in equation (1.3). Even with such a bound, it remains impractical to finish the problem via this approach, since we have no reasonable techniques to obtain a contradiction for a fixed value of n in (1.3), while, as discussed in [3, pp. 34–35], in the case of equation (1.4), we have such a method which is unfortunately computationally infeasible, given the size of our upper bounds for n. For small values of n, however, we have the following result which arises from applying the modular method with the Frey–Hellegouarch curve G.

Table 2.1. Elliptic curves that cannot be eliminated.

q	17	41	89	97
F_q	34a1	82a1	178b1	194a1

Lemma 2.1 ([3, Proposition 14.1]). *Let $q \in \{17, 41, 89, 97\}$ and suppose that (x, k, y, n) is a solution to equation (1.4) with $x \equiv 1 \pmod 4$ and $n \geq 7$ prime. Then $n > 1000$ or (q, x, y, k, n) is one of*

$$(17, -71, 2, 1, 7),\ (41, 13, 2, 0, 7),\ (89, -91, 2, 0, 13)\ \textit{or}\ (97, -15, 2, 0, 7).$$

We note that [3, Proposition 14.1] also provides information on the parity of the exponent k; we will not have use of this.

Proof. When $q \neq 17$, this follows immediately from [3, Proposition 14.1]. For $q = 17$, we use exactly the same method to achieve the desired result. Using [3, Lemma 14.3] deals with all $n > 7$. For the case $n = 7$, we start by applying [3, Lemma 14.6], and following the arguments of [3, pp. 32–34] leaves us needing to solve three Thue–Mahler equations, each of degree 7. To be precise, we need to solve

$$a_7X^7 + a_6X^6Y + a_5X^5Y^2 + a_4X^4Y^3 + a_3X^3Y^4 + a_2X^2Y^5 + a_1XY^6 + a_0Y^7 = 17^k,$$

where $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ is one of

$$(139, 1519, 7119, 18515, 28945, 27069, 14133, 3137),$$
$$(17, 189, 861, 2345, 3395, 3591, 1519, 467)$$

or

$$(1, 189, 14637, 677705, 16679635, 299923911, 2156762783, 11272244723).$$

Using the code and techniques of [10], we find that the first two of these equations yield no solutions, and the third has only the solution $(X, Y) = (1, 0)$, which corresponds to the identity $(-71)^2 - 17^3 = 2^7$. These computations took approximately 2000 seconds for the first equation, and just over one minute for each of the second and third, running Magma V2.24-5 on a 2019 MacBook Pro. ☐

To proceed further, we will now turn our attention to a new Frey–Hellegouarch curve, defined over the real quadratic field $\mathbb{Q}(\sqrt{q})$.

3. Constructing a Frey–Hellegouarch $\mathbb{Q}$-Curve

Let $q \in \{17, 41, 89, 97\}$ and write $M = \mathbb{Q}(\sqrt{q})$. In this section, we construct a new Frey–Hellegouarch curve, this time defined over M. This curve will be a $\mathbb{Q}$-curve, i.e. an elliptic curve, defined over some number field, that is isogenous over $\overline{\mathbb{Q}}$ to all of its Galois conjugates. The $\mathbb{Q}$-curve we define will in fact be *completely defined* over M, meaning that the isogeny between the curve and its conjugate is also defined over M. We will start by following the approach suggested in [3, pp. 47–48].

In each case M has class number 1. We write $\mathcal{O}_M$ for the ring of integers of M. We write σ for the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q})$, and for $z \in M$ we will use the notation $\bar{z} = \sigma(z)$. Although we may suppose that $n > 1000$ by Lemma 2.1, we will for the moment simply assume $n \geq 7$ (and n prime) as in the previous section. We will write δ for a fundamental unit for $\mathcal{O}_M$. For each value of q, the rational prime 2 splits in $\mathcal{O}_M$. Let

$$\gamma = \begin{cases} (-3+\sqrt{q})/2 & \text{if } q = 17, \\ (-19-3\sqrt{q})/2 & \text{if } q = 41, \\ (9+\sqrt{q})/2 & \text{if } q = 89, \\ (325+33\sqrt{q})/2 & \text{if } q = 97. \end{cases}$$

Here, we have chosen γ such that it is a generator for one of the two prime ideals above 2, and such that

$$\gamma\bar{\gamma} = -2, \quad \bar{\gamma} \equiv -1 \pmod{\gamma^2} \quad \text{and} \quad \sqrt{q} \equiv -1 \pmod{\gamma^2}.$$

The relevance of these properties will be seen in due course.

We will now factor the left-hand side of equation (1.4) over M. Writing $y = 2y_1$, we have

$$\left(\frac{x+q^k\sqrt{q}}{2}\right)\left(\frac{x-q^k\sqrt{q}}{2}\right) = 2^{n-2}y_1^n.$$

Since $q \equiv 1 \pmod 4$, each factor on the left-hand side is in $\mathcal{O}_M$. Since $q \nmid x$, we see that

$$\gcd\left(\frac{x+q^k\sqrt{q}}{2}, \frac{x-q^k\sqrt{q}}{2}\right) = 1. \tag{3.1}$$

Now, because $\bar{\gamma} \equiv -1 \pmod{\gamma^2}$ and $x \equiv 1 \pmod 4$, we see that γ must divide $(x+q^k\sqrt{q})/2$, and so $\bar{\gamma}$ will divide $(x-q^k\sqrt{q})/2$. Then by coprimality of the two factors, we have

$$\frac{x+q^k\sqrt{q}}{2} = \delta^r\gamma^{n-2}\alpha^n,$$

for some $r \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_M$. We then obtain that

$$q^k\sqrt{q} = \delta^r\gamma^{n-2}\alpha^n - \bar{\delta}^r\bar{\gamma}^{n-2}\bar{\alpha}^n. \tag{3.2}$$

Treating this equation as a generalized Fermat equation of signature (n,n,n) with solution $(\alpha,\bar{\alpha},1)$ would lead to a Frey–Hellegouarch curve isogenous to the rational Frey–Hellegouarch curve G defined by (2.1). Instead, we will view this as an equation of signature $(n,n,2)$.

Write $k = 2m$ or $2m+1$ according to whether k is even or odd. Let

$$w = \begin{cases} \dfrac{(x + q^{2m}\sqrt{q})}{2} \cdot \sqrt{q}^3 = \delta^r \gamma^{n-2} \alpha^n \sqrt{q}^3 & \text{if } k = 2m, \\ \dfrac{(x + q^{2m+1}\sqrt{q})}{2} \cdot \sqrt{q} = \delta^r \gamma^{n-2} \alpha^n \sqrt{q} & \text{if } k = 2m+1. \end{cases}$$

From equation (3.2), we deduce that

$$\gcd(w, \overline{w}) = \begin{cases} \sqrt{q}^3 & \text{if } k = 2m, \\ \sqrt{q} & \text{if } k = 2m+1. \end{cases}$$

We also have

$$w + \overline{w} = q^{2m+2}.$$

One can attach to any equation of the form $w + \overline{w} = u^2$, with $u \in \mathbb{Q}$, a Frey–Hellegouarch $\mathbb{Q}$-curve; see, by way of example, [12, pp. 199, 203–204]. We take our $\mathbb{Q}$-curve to be

$$E = E_{x,m} = E_{x,m,q} : \ Y^2 = X^3 + 2\gamma q^{m+1} X^2 + \gamma^2 w X. \tag{3.3}$$

This $\mathbb{Q}$-curve is a quadratic twist by γ of the $\mathbb{Q}$-curve one would obtain applying the recipe in [12, p. 199]. The reason for twisting by γ is to ensure the curve E is *completely defined* over M, meaning the isogeny between E and its Galois conjugate is also defined over M. We have

$$\overline{E} = \overline{E}_{x,m} = \overline{E}_{x,m,q} : \ Y^2 = X^3 + 2\overline{\gamma} q^{m+1} X^2 + \overline{\gamma}^2 \overline{w} X, \tag{3.4}$$

and a 2-isogeny, defined over M,

$$\varphi_\sigma : \overline{E} \to E, \quad (X, Y) \mapsto \left(\frac{X^2 + 2\overline{\gamma} q^{m+1} X + \overline{\gamma}^2 \overline{w}}{\overline{\gamma}^2 X}, \frac{(X^2 - \overline{\gamma}^2 \overline{w}) Y}{\overline{\gamma}^3 X^2} \right). \tag{3.5}$$

We would like to compute the conductor $\mathcal{N}_E$ of E. We first note that the curve E has the following standard invariants :

$$c_4 = \gamma^6 \overline{\gamma}^4 (w + 4\overline{w}), \ \ c_6 = \gamma^9 \overline{\gamma}^6 (w - 8\overline{w}) q^{m+1} \quad \text{and} \quad \Delta = \gamma^{12} \overline{\gamma}^6 w^2 \overline{w}.$$

Lemma 3.1. *Let $n \geq 11$. The curve E has multiplicative reduction at both primes of M above 2. As a consequence, E does not have complex multiplication.*

Proof. We recall that γ and $\overline{\gamma}$ generate the two prime ideals of M above 2. The model E is not minimal at these primes, but we will not actually need to write down a minimal model.

We start by noting that $\operatorname{ord}_\gamma(\alpha) = \operatorname{ord}_{\overline{\gamma}}(\overline{\alpha})$. Using (3.1), we also see that $\operatorname{ord}_{\overline{\gamma}}(\alpha) = \operatorname{ord}_\gamma(\overline{\alpha}) = 0$. We then have

$$\operatorname{ord}_\gamma(w) = \operatorname{ord}_{\overline{\gamma}}(\overline{w}) = n - 2 + n \operatorname{ord}_\gamma(\alpha) \ \ \text{and} \ \ \operatorname{ord}_{\overline{\gamma}}(w) = \operatorname{ord}_\gamma(\overline{w}) = 0,$$

whence we deduce that

$$\begin{aligned}
\mathrm{ord}_\gamma(c_4) &= 6 + \mathrm{ord}_\gamma(w + 4\overline{w}) = 8,\\
\mathrm{ord}_\gamma(c_6) &= 9 + \mathrm{ord}_\gamma(w - 8\overline{w}) = 12,\\
\mathrm{ord}_\gamma(\Delta) &= 12 + 2(n - 2 + n\,\mathrm{ord}_\gamma(\alpha)) = 8 + 2n(1 + \mathrm{ord}_\gamma(\alpha)).
\end{aligned}$$

Similarly, we see that

$$\mathrm{ord}_{\overline{\gamma}}(c_4) = 4, \quad \mathrm{ord}_{\overline{\gamma}}(c_6) = 6 \quad \text{and} \quad \mathrm{ord}_{\overline{\gamma}}(\Delta) = 4 + n(1 + \mathrm{ord}_{\overline{\gamma}}(\overline{\alpha})).$$

Writing $j = c_4^3/\Delta$ for the j-invariant of E, we have that

$$\mathrm{ord}_\gamma(j) = 16 - 2n(1 + \mathrm{ord}_\gamma(\alpha)) < 0 \quad \text{and} \quad \mathrm{ord}_{\overline{\gamma}}(j) = 8 - n(1 + \mathrm{ord}_\gamma(\alpha)) < 0,$$

since $n \geq 11$ by assumption. We note that these inequalities will in fact hold whenever $n \geq 9$. We conclude that E has potentially multiplicative reduction at each prime above 2. We can in fact already see at this point that E does not have complex multiplication, since the j-invariant of E is non-integral.

In order to show that E has multiplicative reduction at each prime above 2, it will be enough to prove that the extension $M(\sqrt{-c_6/c_4})/M$ is unramified at γ and $\overline{\gamma}$ (see [9, Lemma 4.3] for example). We have, recalling that $\gamma\overline{\gamma} = -2$,

$$\begin{aligned}
-\frac{c_6}{c_4} &= -\gamma^3\overline{\gamma}^2 \cdot \frac{w - 8\overline{w}}{w + 4\overline{w}} \cdot \sqrt{q}^{2m+2} = -\gamma^3\overline{\gamma}^2 \cdot \frac{w + \gamma^3\overline{\gamma}^3\overline{w}}{w + \gamma^2\overline{\gamma}^2\overline{w}} \cdot \sqrt{q}^{2m+2}\\
&= -\frac{\gamma^4}{\gamma}\overline{\gamma}^2 \cdot \frac{w/\gamma^3 + \overline{\gamma}^3\overline{w}}{w/\gamma^3 + \overline{\gamma}^2\overline{w}/\gamma} \cdot \sqrt{q}^{2m+2} = -(\gamma^2\overline{\gamma}\sqrt{q}^{m+1})^2 \cdot \frac{w/\gamma^3 + \overline{\gamma}^3\overline{w}}{w/\gamma^2 + \overline{\gamma}^2\overline{w}}.
\end{aligned}$$

Write

$$\eta = \gamma^2\overline{\gamma}\sqrt{q}^{m+1} \qquad \text{and} \qquad \kappa = -\frac{w/\gamma^3 + \overline{\gamma}^3\overline{w}}{w/\gamma^2 + \overline{\gamma}^2\overline{w}},$$

so that $M(\sqrt{-c_6/c_4}) = M(\sqrt{\kappa}) = M((1 + \sqrt{\kappa})/2)$.

Consider the numerator of κ. We have that $\mathrm{ord}_\gamma(\overline{\gamma}^3\overline{w}) = 0$, and

$$\mathrm{ord}_\gamma(w/\gamma^3) = n - 2 + n\,\mathrm{ord}_\gamma(\alpha) - 3 = n - 5 + n\,\mathrm{ord}_\gamma(\alpha) \geq 6 > 0,$$

as $n \geq 11$, so γ does not divide the numerator and, similarly for the denominator. So $\mathrm{ord}_\gamma(\kappa) = 0$, and similarly, $\mathrm{ord}_{\overline{\gamma}}(\kappa) = 0$. We have that $\mathrm{ord}_\gamma(w/\gamma^3)$, $\mathrm{ord}_\gamma(w/\gamma^2) > 2$, so $\kappa \equiv -\overline{\gamma} \equiv 1 \pmod{\gamma^2}$ by our choice of γ. We also have that $\kappa \equiv -1/\gamma \equiv 1 \pmod{\overline{\gamma}^2}$ since $\gamma \equiv -1 \pmod{\overline{\gamma}^2}$.

Now, $(1 + \sqrt{\kappa})/2$ satisfies the polynomial

$$X^2 - X + \frac{1 - \kappa}{4}.$$

This polynomial has discriminant κ and is integral at γ and $\overline{\gamma}$. This proves that the extension $M(\sqrt{-c_6/c_4})/M$ is unramified at γ and $\overline{\gamma}$. $\square$

Lemma 3.2. *Let $n \geq 11$.*

(1) *If $\pi \nmid 2q\alpha\overline{\alpha}$ is a prime of M, then E has good reduction at π;*
(2) *If $\pi \nmid 2q$ is a prime of M dividing α or $\overline{\alpha}$, then the model of E is minimal at π, the prime π is of multiplicative reduction for E, and $n \mid \mathrm{ord}_\pi(\Delta)$;*
(3) *E has additive, potentially good reduction at $\sqrt{q}\cdot\mathcal{O}_M$. In particular, we have that $\mathrm{ord}_{\sqrt{q}}(\mathcal{N}_E) = 2$, since $q \geq 5$.*

Proof. Let $\pi \nmid 2q$ be a prime of M. So $\pi \nmid \gamma\overline{\gamma}\sqrt{q}$. If $\pi \nmid \alpha\overline{\alpha}$, then $\pi \nmid \Delta$, so π is a prime of good reduction for E, proving the first part.

Suppose instead that $\pi \nmid 2q$, but that $\pi \mid \alpha\overline{\alpha}$. Then $\pi \mid \Delta$. By (3.1), we see that $\gcd(\alpha, \overline{\alpha}) = 1$. So either $\pi \mid \alpha$ or $\pi \mid \overline{\alpha}$, but not both. So $\pi \mid w$ or $\pi \mid \overline{w}$, but not both. It follows that $\pi \nmid c_4$. So E is minimal at π, and π is a prime of multiplicative reduction for E. Moreover, $\mathrm{ord}_\pi(\Delta) = 2n\,\mathrm{ord}_\pi(\alpha) + n\,\mathrm{ord}_\pi(\overline{\alpha}) \equiv 0 \pmod{n}$, as required.

Finally, we consider $\sqrt{q}$. We have that $\mathrm{ord}_{\sqrt{q}}(w) = \mathrm{ord}_{\sqrt{q}}(\overline{w}) = 1$ or 3 according to whether k is odd or even. So $\mathrm{ord}_{\sqrt{q}}(\Delta) = 3$ or 9, and $\sqrt{q} \mid c_4$. It follows that E is minimal with additive reduction at $\sqrt{q}$. To see that we have potentially good reduction, we show that $\mathrm{ord}_{\sqrt{q}}(j) \geq 0$. We must show that $3\,\mathrm{ord}_{\sqrt{q}}(c_4) \geq \mathrm{ord}_{\sqrt{q}}(\Delta)$, and this inequality holds since

$$\left(\mathrm{ord}_{\sqrt{q}}(\Delta), \mathrm{ord}_{\sqrt{q}}(c_4)\right) = \begin{cases} (9, \geq 3) & \text{if } k \text{ is even,} \\ (3, \geq 1) & \text{if } k \text{ is odd.} \end{cases} \qquad \square$$

Combining Lemmas 3.1 and 3.2, we have that

$$\mathcal{N}_E = \left(\gamma\overline{\gamma}\cdot\sqrt{q}^2\cdot\mathrm{Rad}_2(\alpha\overline{\alpha})\right)\cdot\mathcal{O}_M,$$

where $\mathrm{Rad}_2(\alpha\overline{\alpha})$ denotes the product of all prime ideals of M dividing $\alpha\overline{\alpha}$ but not dividing 2.

4. Irreducibility and Level-Lowering

We would like to apply certain level-lowering results to E in order to relate E to a newform of a particular level and character. We must first prove irreducibility of $\overline{\rho}_{E,n}$, the mod n Galois representation of E. We highlight the fact that we will use the rational Frey–Hellegouarch curve G to help us prove the irreducibility of $\overline{\rho}_{E,n}$.

Proposition 4.1. *Let $q \in \{17, 41, 89, 97\}$. The representation $\overline{\rho}_{E,n}$ is irreducible for $n \geq 11$.*

Proof. Suppose that $\overline{\rho}_{E,n}$ is reducible with $n \geq 11$. If $n = 13$, then arguing as in [12, p. 215], E would give rise to a $\mathbb{Q}(\sqrt{13})$-point on the modular curve $X_0(26)$, a contradiction, since $q \neq 13$. We will therefore suppose that $n = 11$ or $n > 13$. Since E is a $\mathbb{Q}$-curve defined over a quadratic field and the isogeny φ_σ has degree 2, [7, Proposition 3.2] tells us that every prime of M of characteristic > 3 is a prime of potentially good reduction for E.

We first show that y must be a power of 2. If $\ell > 3$ is a prime with $\ell \mid y$, then each prime of M above ℓ will divide either α or $\overline{\alpha}$, and it follows (by Lemma 3.2) that we have a prime of characteristic $\ell > 3$ of multiplicative reduction for E, a contradiction. Next, suppose that $3 \mid y$. Then 3 is a prime of multiplicative reduction for the rational Frey–Hellegouarch curve G defined in (2.1). From the isomorphism $\bar{\rho}_{G,n} \sim \bar{\rho}_{F,n}$, for F an elliptic curve of level $2q$ in Table 2.1, we have, writing f for the newform corresponding to F, that

$$n \mid 3 + 1 \pm a_3(f). \tag{4.1}$$

From the Hasse bound, we have that $|a_3(f)| \leq 2\sqrt{3}$ and hence the right-hand-side of (4.1) is a nonzero integer, bounded above by $4 + 2\sqrt{3}$. This contradicts $n \geq 11$ and so we may conclude that y is necessarily a power of 2, say $y = 2^s$, with $s \geq 1$ since y is even.

We thus have that $x^2 - 2^{ns} = q^{2k+1}$. By [11, p. 328], this equation has no solutions with $n \geq 11$, provided $2k + 1 > 1$. It follows that $k = 0$ and we have

$$x^2 = 2^{ns} + q.$$

Multiplying both sides by 2^2 or 2^4 if necessary, we obtain an integral point on one of the following elliptic curves:

$$Y^2 = X^3 + q, \quad Y^2 = X^3 + 2^2 q \quad \text{or} \quad Y^2 = X^3 + 2^4 q.$$

Computing the integral points on each of these curves for each value of q using `Magma` quickly leads to a contradiction. $\square$

Remark 4.2. At this point, we could apply standard level-lowering results over M (see [8, Theorem 7] for example) to relate $\bar{\rho}_{E,n}$ to the Galois representation of a Hilbert newform at level $\gamma\bar{\gamma}\sqrt{q}^2 \cdot \mathcal{O}_M$. For $q = 17, 41, 89$, and 97, the dimensions of these spaces of newforms are $46, 1093, 9631$, and 26378 respectively. Computing the newform data at these levels using `Magma` is certainly possible for $q = 17$, and would also likely be achievable for $q = 41$ by working directly with Hecke operators (see [13, p. 342–343] for example), but for $q = 89$, and especially for $q = 97$, the dimensions are likely too large for current computations. The $\mathbb{Q}$-curve approach we now present will allow us to work with classical modular forms and make the resulting computations feasible.

We start by computing some data associated to the $\mathbb{Q}$-curve E, which we recall does not have complex multiplication (by Lemma 3.1). We will use the notation and terminology of Quer [15]. We note that we are in a similar set-up to that of [2, pp. 8–9]. As in the previous section, we write $\mathrm{Gal}(M/\mathbb{Q}) = \{1, \sigma\}$. We have the isogeny $\varphi_\sigma : \overline{E} \to E$ given by (3.5), and

φ_1 will denote the identity morphism on E. Write $c : \mathrm{Gal}(M/\mathbb{Q}) \to \mathbb{Q}^*$ for the 2-cocycle given by

$$c(s,t) = \varphi_s \, {}^s\varphi_t \, \varphi_{st}^{-1}.$$

We have that $c(1,1) = c(1,\sigma) = c(\sigma,1) = 1$. By a direct computation with `Magma`, we verify that $c(\sigma,\sigma) = \varphi_\sigma({}^\sigma\varphi_\sigma) = -2$.

Next, define

$$\beta : \mathrm{Gal}(M/\mathbb{Q}) \to \overline{\mathbb{Q}}^*, \qquad \beta(1) = 1, \ \beta(\sigma) = \sqrt{-2}.$$

This map satisfies

$$c(s,t) = \beta(s)\beta(t)\beta(st)^{-1} \quad \text{for } s,t \in \mathrm{Gal}(M/\mathbb{Q}). \tag{4.2}$$

It follows that β is a *splitting map* for c (as defined in [15, p. 298]). The *splitting character* associated to β is then defined by

$$\epsilon(s) = \beta(s)^2 / \deg(\varphi_s).$$

So $\epsilon(1) = 1$ and $\epsilon(\sigma) = -1$, and ϵ is the quadratic Galois character associated to M. Since $q \equiv 1 \pmod 4$, we have $M \subset \mathbb{Q}(\zeta_q)$, and we may also view ϵ as a quadratic Dirichlet character $\epsilon : (\mathbb{Z}/q\mathbb{Z})^\times \to \{\pm 1\}$ of conductor q via $(\mathbb{Z}/q\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \to \mathrm{Gal}(M/\mathbb{Q})$.

Write $B = \mathrm{Res}_{\mathbb{Q}}^M(E)$ for the restriction of scalars of E to $\mathbb{Q}$. This is an abelian surface defined over $\mathbb{Q}$ and plays an important role. The relation (4.2) shows that the 2-cocycle c has trivial Schur class (i.e. is trivial when viewed as an element of $H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}}^*)$ with trivial action). By [15, Proposition 5.2], we deduce that B decomposes as a product of abelian varieties of GL_2-type. Moreover, the $\mathbb{Q}$-simple abelian variety of GL_2-type, A_β, attached to β, which is a quotient of B, will have endomorphism algebra $\mathbb{Q}(\beta(1), \beta(\sigma)) = \mathbb{Q}(\sqrt{-2})$ (see [15, pp. 305–306]), and is therefore itself an abelian surface. It follows that B is $\mathbb{Q}$-isogenous to A_β, so B is $\mathbb{Q}$-simple and of GL_2-type with $\mathbb{Q}$-endomorphism algebra $\mathbb{Q}(\sqrt{-2})$. We record this in the following proposition.

Proposition 4.3. *The abelian surface $B = \mathrm{Res}_{\mathbb{Q}}^M(E)$ is $\mathbb{Q}$-simple and of GL_2-type. It has $\mathbb{Q}$-endomorphism algebra $\mathbb{Q}(\sqrt{-2})$. The conductor of B is given by*

$$N_B = \left(2q^2 \, \mathrm{Rad}_2(y)\right)^2.$$

Proof. It remains to compute the conductor of B. This can be obtained from the conductor of E using the formula in [14, Proposition 1]. Writing Δ_M for the discriminant of M, we have

$$N_B = (\Delta_M)^2 \, \mathrm{Norm}(\mathcal{N}_E) = q^2 \cdot 2^2 q^2 \cdot \mathrm{Norm}(\mathrm{Rad}_2(\alpha\overline{\alpha})) = 2^2 q^4 (\mathrm{Rad}_2(y))^2,$$

and the proposition follows. □

We can now use the modularity of B and standard level-lowering results to deduce the following result.

Proposition 4.4. *Let $q \in \{17, 41, 89, 97\}$ and let $n \geq 11$ with $n \neq q$. Write $G_M = \mathrm{Gal}(\overline{\mathbb{Q}}/M)$. Then we have*

$$\bar{\rho}_{E,n} \sim \bar{\rho}_{f,\mathfrak{n}}|_{G_M}, \tag{4.3}$$

for f a newform of level $2q^2$ and character ϵ, and $\mathfrak{n}$ a prime above n in the coefficient field of f.

Proof. By [16, Theorem 4.4], B is isogenous to a factor, A_g, of $J_1(N)$ for some N, where A_g is the abelian variety attached to some newform g. We have that $N^{\dim(A_g)} = N_B = \left(2q^2 \,\mathrm{Rad}_2(y)\right)^2$, and so $N = 2q^2 \,\mathrm{Rad}_2(y)$. Moreover, g has character $\epsilon^{-1} = \epsilon$, since ϵ has order 2.

By Proposition 4.1, the representation $\bar{\rho}_{E,n}$ is irreducible, so the representation $\bar{\rho}_{g,\pi}$ is too, and applying standard level-lowering results, we have that $\bar{\rho}_{g,\pi} \sim \bar{\rho}_{f,\mathfrak{n}}$, for f a newform of level $2q^2$ and character ϵ, and $\pi, \mathfrak{n}$ primes above n. Since $\beta|_{G_M}$ is trivial, using [12, pp. 210–211], we have

$$\bar{\rho}_{E,n} \sim \bar{\rho}_{g,\pi}|_{G_M} \sim \bar{\rho}_{f,\mathfrak{n}}|_{G_M},$$

as required. ☐

5. Eliminating Newforms

We start by using `Magma` to compute the Galois conjugacy classes of newforms (i.e. their q-expansions) at level $2q^2$ with character ϵ. Table 5.1 records some of this data.

TABLE 5.1. Newform data. Here, *dim* refers to the dimension of the space of newforms and *time* refers to the computation time using a 2200MHz AMD Opterons.

q	dim	no. classes	(size of class, multiplicity)	time
17	22	6	$(2,3),(4,1),(6,2)$	1 s
41	136	18	$(2,4),(4,5),(6,2),(8,4),(16,1),(24,2)$	8 s
89	652	26	$(2,4),(4,2),(6,4),(8,3),(12,2),(24,3),(30,1),$ $(40,2),(50,1),(60,1),(80,1),(96,2)$	400 s
97	774	29	$(2,4),(4,3),(6,3),(8,4),(12,3),(20,3),(24,1),$ $(32,3),(40,1),(48,1),(64,1),(168,2)$	739 s

Let $\mathfrak{p} \nmid 2qn$ be a prime of M above a rational prime p and denote by $\mathrm{Frob}_{\mathfrak{p}} \in G_M$ a Frobenius element at $\mathfrak{p}$. Let f denote the newform related to E in Proposition 4.4. Then, taking traces in (4.3), we have

$$\mathrm{Tr}(\bar{\rho}_{E,n}(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{Tr}(\bar{\rho}_{f,\mathfrak{n}}(\mathrm{Frob}_{\mathfrak{p}})). \tag{5.1}$$

We first consider the right-hand side of (5.1). Writing $a_p(f)$ for the p-th coefficient of the q-expansion of f, we start by defining the quantity

$$t_{f,\mathfrak{p}} = \begin{cases} a_p(f) & \text{if } p \text{ splits in } M, \\ a_p(f)^2 + 2p & \text{if } p \text{ is inert in } M. \end{cases}$$

By [12, pp. 217–219] for example, we have $\mathrm{Tr}(\bar{\rho}_{f,\mathfrak{n}}(\mathrm{Frob}_{\mathfrak{p}})) \equiv t_{f,\mathfrak{p}} \pmod{\mathfrak{n}}$, where we have used the fact that $\epsilon(p) = -1$ when p is inert in M. We highlight the fact that $t_{f,\mathfrak{p}}$ is independent of $\mathfrak{n}$.

Next, for the left-hand side of (5.1), the quantity $\mathrm{Tr}(\bar{\rho}_{E,n}(\mathrm{Frob}_{\mathfrak{p}}))$ is dependent on our choice of x and m (i.e. dependent on our original solution to equation (1.4)). However, looking at how $E = E_{x,m}$ is defined in (3.3), we see that the trace will only depend on x and $q^m \pmod{p}$. In particular, it will only depend on the value of x modulo p, and m modulo $(p-1)$ (in fact it will only depend on m modulo the multiplicative order of $q \pmod{p}$). Given $0 \le \chi \le p-1$ and $0 \le \mu \le p-2$, write $E_{\chi,\mu}$ for the curve obtained by substituting $x = \chi$ and $m = \mu$ into $E_{x,m}$, defined in (3.3). If $\mathfrak{p} \mid \Delta_{E_{\chi,\mu}}$ then, as in the proof of Lemma 3.2 (2), we see that $\mathfrak{p} \nmid c_4(E_{\chi,\mu})$ (and also $\mathfrak{p} \nmid c_6(E_{\chi,\mu})$), so $E_{\chi,\mu}$ has multiplicative reduction at $\mathfrak{p}$. We then have

$$\begin{aligned} &\mathrm{Tr}(\bar{\rho}_{E_{\chi,\mu},n}(\mathrm{Frob}_{\mathfrak{p}})) \\ &\qquad = \begin{cases} a_{\mathfrak{p}}(E_{\chi,\mu}) & \text{if } \ \mathfrak{p} \nmid \Delta_{E_{\chi,\mu}}, \\ \mathrm{Norm}(\mathfrak{p}) + 1 & \text{if } \ \mathfrak{p} \mid \Delta_{E_{\chi,\mu}} \text{ and } (-c_6/c_4 \bmod \mathfrak{p}) \in (\mathbb{F}_{\mathfrak{p}}^*)^2, \\ -\mathrm{Norm}(\mathfrak{p}) - 1 & \text{if } \ \mathfrak{p} \mid \Delta_{E_{\chi,\mu}} \text{ and } (-c_6/c_4 \bmod \mathfrak{p}) \notin (\mathbb{F}_{\mathfrak{p}}^*)^2. \end{cases} \end{aligned}$$

We can now simply run through all possible pairs χ and μ in this range. Define

$$\mathcal{A}_{\mathfrak{p}} = \{\mathrm{Tr}(\bar{\rho}_{E_{\chi,\mu},n}(\mathrm{Frob}_{\mathfrak{p}})) : 0 \le \chi \le p-1, \quad 0 \le \mu \le p-2\}.$$

Then we know that $\mathrm{Tr}(\bar{\rho}_{E_{x,m},n}(\mathrm{Frob}_{\mathfrak{p}})) \in \mathcal{A}_{\mathfrak{p}}$, and we can compute the set $\mathcal{A}_{\mathfrak{p}}$ for any $\mathfrak{p} \nmid 2qn$.

Define

$$\mathcal{B}_{f,\mathfrak{p}} = p \cdot \mathrm{Norm}\left(\prod_{a \in \mathcal{A}_{\mathfrak{p}}} (a - t_{f,\mathfrak{p}})\right).$$

Then by (5.1) we have that $n \mid \mathcal{B}_{f,\mathfrak{p}}$ whenever $\mathfrak{p} \nmid 2q$. Note that we have included a factor of p in the definition of $\mathcal{B}_{f,\mathfrak{p}}$, as we would usually require $\mathfrak{p} \nmid 2qn$, but n is unknown. Then if $\mathcal{B}_{f,\mathfrak{p}}$ is non-zero, we obtain a bound on

n. Moreover, we can repeat this with many auxiliary primes $\mathfrak{p}$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are primes not dividing $2q$, then

$$n \mid \mathcal{B}_f = \mathcal{B}_{f,\mathfrak{p}_1,\ldots,\mathfrak{p}_r} = \gcd\left(\mathcal{B}_{f,\mathfrak{p}_1}, \ldots, \mathcal{B}_{f,\mathfrak{p}_r}\right).$$

Proof of Theorem 1.1. Let $q = 41$ or 97. We computed the value $\mathcal{B}_f$, and in particular its prime factors, for each newform f at level $2q^2$ and character ϵ. For most newforms f, we did this by choosing a prime of M above each rational prime between 3 and 30. For computational reasons, when $q = 97$ and f is one of the two newforms with coefficient field of degree 168, we only worked with a prime above each of 3 and 11. We found that for each newform f, all prime factors of $\mathcal{B}_f$ were < 300, except for two newforms when $q = 41$, which we denote g_1 and g_2. Since we can take $n > 1000$ by Lemma 2.1, this eliminates all newforms except for g_1 and g_2. We are unable to eliminate these two newforms as their $\mathcal{B}$ values are 0, and this remains the case when using more auxiliary primes.

Since we managed to eliminate all newforms when $q = 97$, this proves Theorem 1.1 in the case $q = 97$. For $q = 41$, we are able to eliminate the remaining forms using a multi-Frey approach.

Let $q = 41$. Recall that $k = 2m$ or $2m+1$ according to whether k is even or odd, respectively. From Table 2.1, we know that $\bar{\rho}_{G_{x,k,q},n} \sim \bar{\rho}_{F,n}$ where F is the elliptic curve with Cremona label '82a1'. Let $p = 7$ which is inert in M, and write $\mathfrak{p} = p \cdot \mathcal{O}_M$ for the unique prime of M above 7.

We compute $a_7(F) = -4$. Given $0 \le \chi \le 6$ and $0 \le \kappa \le 5$, write $G_{\chi,\kappa}$ for the curve obtained by substituting $x = \chi$ and $k = \kappa$ into the definition of $G_{x,k,q}$ in (2.1). Then we compute $\mathrm{Tr}(\bar{\rho}_{G_{\chi,\kappa},n}(\mathrm{Frob}_7))$ for each χ and κ. We found this trace to be independent of κ. The traces are recorded in Table 5.2 and we see that this forces $x \equiv 6 \pmod 7$.

Table 5.2. Proof of Theorem 1.1: Traces of Frobenius at 7 for G.

χ	0	1	2	3	4	5	6
$\mathrm{Tr}(\bar{\rho}_{G_{\chi,\mu},n}(\mathrm{Frob}_7))$	0	4	2	2	-2	-2	-4

When $\chi = 6$, we find that $\mathrm{Tr}(\bar{\rho}_{E_{6,\mu},n}(\mathrm{Frob}_\mathfrak{p})) = 6$ for each $0 \le \mu \le 5$ and k even or odd. However,

$$\mathrm{Tr}(\bar{\rho}_{g_1,\mathfrak{n}_1}(\mathrm{Frob}_\mathfrak{p})) = a_p(g_1)^2 + 2p = -4, \text{ and}$$
$$\mathrm{Tr}(\bar{\rho}_{g_2,\mathfrak{n}_2}(\mathrm{Frob}_\mathfrak{p})) = a_p(g_2)^2 + 2p = 14.$$

It follows that $n \mid 7 \cdot 10$ or $n \mid 7 \cdot 12$. So $x \not\equiv 6 \pmod 7$, a contradiction. This completes the proof of the theorem. □

When $q = 17$ or $q = 89$, we found that, in each case, there was a single obstructing newform that we were unable to eliminate. When $q = 17$, this is due to the solution $(-23)^2 - 17 = 2^9$, and when $q = 89$, this is a consequence of the identity $(-91)^2 - 89 = 2^{13}$. The exponent n in each case exceeds 8, and it follows that the curves $E_{-23,0,17}$ and $E_{-91,0,89}$ have multiplicative reduction at the primes of M above 2. This can be verified directly or can be seen from the proof of Lemma 3.1. We can check that the traces of Frobenius for these two curves match the traces of the obstructing newforms (for all primes of characteristic < 1000 say). We also note that in both cases, the coefficient field of the obstructing newform is $\mathbb{Q}(\sqrt{-2})$. This is the same as the $\mathbb{Q}$-endomorphism algebra of $B = \mathrm{Res}^M_{\mathbb{Q}}(E)$, as expected.

When $q = 41$ or $q = 97$, the solutions in Theorem 1.1 with exponent $n = 7$ prevent us from eliminating the isomorphism of mod n representations of G and F_q (as noted in Section 2), but these solutions do not pose any issue when working with the $\mathbb{Q}$-curve E. This is because the exponent $n = 7$ is not large enough to force multiplicative reduction at the primes of M above the rational prime 2. A similar remark applies for (restricting attention to primes $q < 1000$)

$$q \in \{233, 313, 401, 601\},$$

which are potentially accessible to the methods of this paper (though the corresponding computation of forms at level $2q^2$ would, with current techniques, be formidable).

References

[1] C. Barros, "On the Lebesgue–Nagell equation and related subjects", PhD Thesis, University of Warwick, 2010.

[2] M. A. Bennett, I. Chen, S. R. Dahmen & S. Yazdani, "On the equation $a^3 + b^{3n} = c^2$", *Acta Arith.* **163** (2014), no. 4, p. 327-343.

[3] M. A. Bennett & S. Siksek, "Differences between perfect powers: prime power gaps", `https://arxiv.org/abs/2110.05553v1`, to appear in *Algebra Number Theory*, 2021.

[4] ———, "Differences between perfect powers: the Lebesgue–Nagell equation", *Trans. Am. Math. Soc.* **3776** (2023), no. 1, p. 335-370.

[5] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.

[6] Y. Bugeaud, "On the Diophantine equation $x^2 - p^m = \pm y^n$", *Acta Arith.* **80** (1997), no. 3, p. 213-223.

[7] J. S. Ellenberg, "Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$", *Am. J. Math.* **126** (2004), no. 4, p. 763-787.

[8] N. Freitas & S. Siksek, "The asymptotic Fermat's last theorem for five-sixths of real quadratic fields", *Compos. Math.* **151** (2015), no. 8, p. 1395-1415.

[9] ———, "Fermat's last theorem over some small real quadratic fields", *Algebra Number Theory* **9** (2015), no. 4, p. 875-895.

[10] A. Gherga & S. Siksek, "Efficient resolution of Thue–Mahler equations", `https://arxiv.org/abs/2207.14492v1`, 2022.

[11] W. Ivorra, "Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$", *Acta Arith.* **108** (2003), no. 4, p. 326-338.

[12] J. M. van Langen, "On the sum of fourth powers in arithmetic progressions", *Int. J. Number Theory* **17** (2021), no. 1, p. 191-221.

[13] P. Michaud-Jacobs, “Fermat’s Last Theorem and modular curves over real quadratic fields”, *Acta Arith.* **203** (2022), no. 4, p. 319-352.
[14] J. S. Milne, “On the arithmetic of abelian varieties”, *Invent. Math.* **17** (1972), p. 177-190.
[15] J. Quer, “$\mathbb{Q}$-Curves and abelian varieties of GL_2-type”, *Proc. Lond. Math. Soc.* **81** (2000), no. 2, p. 285-317.
[16] K. A. Ribet, “Abelian varieties over $\mathbb{Q}$ and modular forms”, in *Algebra and Topology 1992*, Korea Advanced Institute of Science and Technology, Mathematics Research Center, 1992, p. 53-79.

Michael A. Bennett
Department of Mathematics
University of British Columbia
Vancouver, B.C., V6T 1Z2, Canada
E-mail: `bennett@math.ubc.ca`
URL: `https://personal.math.ubc.ca/~bennett/`

Philippe Michaud-Jacobs
Mathematics Institute
University of Warwick
Coventry CV4 7AL, United Kingdom
E-mail: `p.rodgers@warwick.ac.uk`
URL: `https://warwick.ac.uk/fac/sci/maths/people/staff/michaud/`

Samir Siksek
Mathematics Institute
University of Warwick
Coventry CV4 7AL, United Kingdom
E-mail: `s.siksek@warwick.ac.uk`
URL: `https://homepages.warwick.ac.uk/~maseap/`