# A MULTI-FREY APPROACH TO SOME MULTI-PARAMETER FAMILIES OF DIOPHANTINE EQUATIONS

YANN BUGEAUD, MAURICE MIGNOTTE, SAMIR SIKSEK

Abstract. We solve several multi-parameter families of binomial Thue equations of arbitrary degree; for example, we solve the equation

$$5^u x^n - 2^r 3^s y^n = \pm 1,$$

in non-zero integers $x$, $y$ and positive integers $u$, $r$, $s$ and $n \geq 3$. Our approach uses several Frey curves simultaneously, Galois representations and level-lowering, new lower bounds for linear forms in 3 logarithms due to Mignotte and a famous theorem of Bennett on binomial Thue equations.

## 1. Introduction

The most radical idea in the recent study of Diophantine equations has been the introduction of the 'Frey curve' [16], [17]. This has lead to the resolution of many infamous Diophantine problems; most notable among these is Wiles' proof of Fermat's Last Theorem [33], [31].

In this paper we demonstrate, by way of example, that the simultaneous use of several Frey curves—when available—is an even more powerful tool for the study of Diophantine equations. This 'multi-Frey' approach often resolves with ease equations that would otherwise seem utterly hopeless.

We illustrate our purpose by completely solving several multi-parametric families of Thue equations. There is a broad literature on this topic, starting from the pioneering work of Thomas [32]. Authors were mainly concerned with one- or two-parametric families of Thue equations of *fixed* degree; see for example [18] for a survey. However, in a remarkable paper [2], Bennett solves an infinite family of Thue equations of arbitrary degree using the hypergeometric method and linear forms in logarithms. Indeed, he showed that if $b$, $n$ are integers with $b \neq 0, -1$ and $n \geq 3$, then the equation

$$|(b+1)x^n - by^n| = 1$$

has exactly one solution in positive integers $x$, $y$, which is given by $x = y = 1$.

As in Bennett's theorem, our main results concern binary Thue equations of arbitrary degree.

**Theorem 1.** *Suppose $3 \leq q < 100$ is a prime. The solutions to the equation*

$$q^u x^n - 2^r y^n = \pm 1, \qquad x,\ y \text{ non-zero integers}, \quad u,\ r \geq 0, \quad n \geq 3 \tag{1}$$

*Date*: April 20, 2006.

2000 *Mathematics Subject Classification.* Primary 11F80, 11D61, Secondary 11D59, 11J86, 11Y50.

*Key words and phrases.* Diophantine equations, Frey curves, level-lowering, linear forms in logarithms, Thue equations.

Y. Bugeaud's work is supported by the Austrian Science Foundation FWF, grant M822-N12. S. Siksek's work is funded by a grant from Sultan Qaboos University (IG/SCI/DOMS/02/06).

*are given in Table 8.*

**Theorem 2.** *Suppose $3 \le q_2 < q_1 \le 31$ are primes. The solutions to the equation*

$$q_1^u x^n - q_2^v y^n = \pm 1, \qquad x,\ y \text{ non-zero integers}, \quad u,\ v \ge 0, \quad n \ge 3 \tag{2}$$

*are given in Table 9.*

**Theorem 3.** *Suppose $q = 5$ or $7$. The solutions to the equation*

$$q^u x^n - 2^r 3^s y^n = \pm 1, \qquad x,\ y \text{ non-zero integers}, \quad u,\ r,\ s > 0, \quad n \ge 3 \tag{3}$$

*are given in Table 10.*

The reader will note that equations (1), (2) involve 5 unknowns, whereas equation (3) involves 6 unknowns. Moreover, many of these equations have non-trivial solutions.

Our tools for proving Theorems 1–3, apart from the multi-Frey approach, are a recent estimate for linear forms in three logarithms by Mignotte [24], and the aforementioned theorem of Bennett. Of course, to apply the multi-Frey approach one has to assume—just as in the Frey approach—the modularity of elliptic curves proved by Wiles and others [33], [31], [11], [15], [8], Ribet's Level-Lowering Theorem [25], and results on the irreducibility of Galois representations due to Mazur and others [23].

We note in passing that a recent paper of Bennett [3] solves equations of the form $ax^n - by^n = \pm 1$ where $ab = 2^r 3^s$. Bennett's approach uses three Frey curves, but it is not multi-Frey in our sense. We call Bennett's approach in [3] 'repeated single-Frey' and we explain the difference between the two approaches in Section 5.

We are indebted to the referee for several insightful comments. We warmly thank the 'Centre de Calcul MEDICIS' at the École Polytechnique, where most of the computation have been done.

## 2. Essential Definitions and Notation

2.1. **Newforms and Galois Representations.** By a newform of level $N$ we mean a normalized cuspidal eigenform of weight 2 and belonging to the new space at level $N$. We shall think of newforms in terms of their $q$-expansions around infinity and write them thus:

$$f = q + \sum_{n \ge 2} c_n q^n. \tag{4}$$

As is well-known, the coefficients $c_n$ generate a finite extension $K/\mathbb{Q}$ that is totally real, and moreover these coefficients are all algebraic integers. If $K = \mathbb{Q}$, we say that the newform $f$ is rational, otherwise we say it is irrational.

For an elliptic curve $E$, and for prime $l$ of good reduction for $E$, we write $\sharp E(\mathbb{F}_l)$ for the number of points on $E$ over the finite field $\mathbb{F}_l$, and let $a_l(E) = l + 1 - \sharp E(\mathbb{F}_l)$.

**Notation.** *Suppose $E$ is an elliptic curve, $f$ is a newform and $p$ a prime. We write $E \sim_p f$ if the Galois representation on the $p$-torsion of $E$ arises from $f$.*

*Suppose $E_1, \ldots, E_n$ are elliptic curves, $f_1, \ldots, f_n$ are newforms, and again $p$ is a prime. Write $\mathfrak{E}$ and $\mathfrak{f}$ for the $n$-tuples $\mathfrak{E} = (E_1, \ldots, E_n)$ and $\mathfrak{f} = (f_1, \ldots, f_n)$. By $\mathfrak{E} \sim_p \mathfrak{f}$ we simply mean that $E_i \sim_p f_i$ for $i = 1, \ldots, n$.*

The following lemma is perfectly standard; see [28, page 196], [4, page 7], [20, Proposition 5.4] for the first part, and [21, Prop. 3] for the second part.

**Lemma 2.1.** *Suppose $f$ is a newform of level $N$ represented by a $q$-expansion as in (4), with coefficients generating a number field $K$. Suppose $E$ is an elliptic curve over $\mathbb{Q}$ of conductor $N'$ with $E \sim_p f$. Then there is some prime ideal $\mathfrak{p}$ of $K$ such that $\mathfrak{p} \mid p$ and for all primes $l$,*

(a) *if $l \nmid pNN'$ then $a_l(E) \equiv c_l \pmod{\mathfrak{p}}$,*
(b) *if $l \nmid pN$ but $l \parallel N'$ then $\pm(l+1) \equiv c_l \pmod{\mathfrak{p}}$.*

*Moreover, if $f$ is rational, then the above can be relaxed slightly as follows: for all primes $l$,*

(a′) *if $l \nmid NN'$ then $a_l(E) \equiv c_l \pmod{p}$,*
(b′) *if $l \nmid N$ but $l \parallel N'$ then $\pm(l+1) \equiv c_l \pmod{p}$.*

Notice that in the second part of the Lemma, where $f$ is supposed to be rational, we do not exclude the case $l = p$. We shall also need the following result of Kraus on congruences of newforms.

**Proposition 2.2.** *(Kraus [19]) Suppose $f$ is a newform of level $N$ with $q$-expansion as in (4). Let $K = \mathbb{Q}(c_2, c_3, \ldots)$ be the number field generated by the coefficients $c_n$ appearing in the $q$-expansion of $f$. Let*

$$M = \operatorname{lcm}(4, N), \qquad \mu(M) = M \prod_{\substack{q \mid M, \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right).$$

*Suppose that $\mathfrak{p}$ is a prime ideal of $K$ such that the following two conditions hold:*

(i) *for every prime $l \leq \mu(M)/6$, $l \nmid 2N$, we have*
$$l + 1 \equiv c_l \pmod{\mathfrak{p}};$$
(ii) *for every prime $l \leq \mu(M)/6$, $l \mid 2N$, $l^2 \nmid 4N$, we have*
$$(l+1)(c_l - 1) \equiv 0 \pmod{\mathfrak{p}}.$$

*Then for every prime number $l \nmid 2N$ we have $l + 1 \equiv c_l \pmod{\mathfrak{p}}$.*

2.2. **Elliptic Surfaces.** The Frey curves that we present later are most conveniently thought of as elliptic curves over the field $\mathbb{Q}(\Psi)$.

If $k$ is a field, then an elliptic curve $E_\Psi$ over the field $k(\Psi)$ naturally defines a fibered elliptic surface $\mathcal{E} \to \mathbb{A}^1$ (note that we disregard the fiber at infinity). If $\psi \in k$, we write $E_\psi$ for the fiber at $\psi$; this is simply obtained by replacing $\Psi$ with $\psi$. The generic fiber of $\mathcal{E} \to \mathbb{A}^1$ is just our original curve $E_\Psi$ over $k(\Psi)$.

**Definition.** *Let $S$ be a finite set of primes. By an $S$-integral elliptic surface we mean a fibered elliptic surface $\mathcal{E} \to \mathbb{A}^1$ defined over $\mathbb{Q}$ whose generic fiber $E_\Psi$ is given by a Weierstrass equation with coefficients in $\mathbb{Z}_S[\Psi]$. If $\mathcal{E} \to \mathbb{A}^1$ is an $S$-integral elliptic surface and $l \notin S$ is a prime, and if the curve $E_\phi/\mathbb{F}_l$ is non-singular or nodal for all $\phi \in \mathbb{F}_l$, then we shall say that $l$ is a prime of moderate reduction for $\mathcal{E} \to \mathbb{A}^1$.*

It will be convenient to drop the distinction between the surface $\mathcal{E} \to \mathbb{A}^1$ and its generic fiber $E_\Psi$ and simply call $E_\Psi$ an elliptic surface. The following elementary Lemma will be useful.

**Lemma 2.3.** *Let $S$ be a finite set of primes and suppose $E_\Psi$ is an $S$-integral elliptic surface. Write $c_4$, $\Delta$ for the usual quantities associated to the Weierstrass model, and let $R$ be their resultant (regarded as polynomials in $\Psi$). If $l \notin S$ is a prime such that $\operatorname{ord}_l(R) = 0$, then $l$ is a prime of moderate reduction for $E_\Psi$.*

## 3. Frey Curves (or Surfaces)

In this section we apply the modular approach to the equations (1)–(3) under suitable, but mild, hypotheses. Ordinarily, one would have to construct a Frey curve or curves associated to our equation, show that the Galois representation is irreducible (under suitable hypotheses) using the results of Mazur and others [23], and modular by the work of Wiles and others [33], [31], [11], [15], [8], and finally apply Ribet's Level-Lowering Theorem [25]. However, one sees that any equation of the form (1)–(3) is a special case of each of the equations $Ax^n + By^n + Cz^n = 0$, $Ax^n + By^n = Cz^2$ and $Ax^n + By^n = Cz^3$. Fortunately, suitable Frey curves and the details of level-lowering have been worked out for these equations respectively by Kraus [19], Bennett and Skinner [4], and Bennett, Vatsal and Yazdani [5]; we have merely applied their recipes. It is however convenient to change notation a little, so as to be able to deal with equations (1)–(3) in a uniform way. Before doing this we remark that for small exponents, equations (1)–(3) can be solved using standard techniques for Thue equations [6]; these techniques are implemented in the computer algebra system `MAGMA` [7] and we did use them to solve equations (1)–(3) for exponents $n = 3$, 4, 5 (observe that there is no restriction in assuming that the exponents $u, r, s, v$ are smaller than $n$). Hence there is no harm in assuming that the exponent $n$ is a prime $\geq 7$.

We concern ourselves in this section with the equation

$$\alpha x^p - 2^r \beta y^p = 1, \tag{5}$$

where

$$\alpha,\ \beta \text{ are non-zero, coprime and odd,} \tag{6}$$

$$0 \leq \mathrm{ord}_q\, \alpha, \mathrm{ord}_q\, \beta < p \quad \text{for all primes } q. \tag{7}$$

We furthermore restrict our attention to solutions $(p, r, x, y)$ satisfying the following conditions

$$p \geq 7 \text{ is prime}, \qquad 0 \leq r < p, \tag{8}$$

$$x,\ y \text{ are non-zero integers} \tag{9}$$

$$\text{either } r > 0 \text{ or } y \text{ is even}, \tag{10}$$

$$2^r \beta y^p \neq \pm 2. \tag{11}$$

The conditions $p \geq 7$ and $2^r \beta y^p \neq \pm 2$ are needed later on to ensure the irreducibility of the Galois representations on the $p$-torsion of the Frey curves.

We shall associate our putative solution of equation (5) to three different Frey curves (or surfaces depending on our point of view), one from each of the following families that we now introduce. The 'F-family':

$$F^1_\Psi: \quad Y^2 = X^3 + (2\Psi + 1)X^2 + (\Psi^2 + \Psi)X,$$

$$F^2_\Psi: \quad Y^2 = X^3 - (2\Psi + 1)X^2 + (\Psi^2 + \Psi)X.$$

The 'G-family':

$$G^1_\Psi: \quad Y^2 + XY = X^3 - \frac{\Psi}{64}X, \qquad G^2_\Psi: \quad Y^2 = X^3 + X^2 - \frac{\Psi}{4}X,$$

$$G^3_\Psi: \quad Y^2 = X^3 - X^2 - \frac{\Psi}{4}X, \qquad G^4_\Psi: \quad Y^2 = X^3 + 2X^2 - \Psi X.$$

TABLE 1. Frey Curves of the F- and G-Family

| Case | Conditions on $r$ and/or $y$ | F-Frey curve | $L_1$ | G-Frey curve | $L_2$ |
|---|---|---|---|---|---|
| (I) | $y$ even and $r \neq 4,\ 6$ or $y$ odd and $r \geq 7$ | $F^1_\Psi$ | 2 | $G^1_\Psi$ | 2 |
| (II) | $y$ even and $r = 4$ | $F^1_\Psi$ | 1 | $G^1_\Psi$ | 2 |
| (III) | $r = 6$ | $F^1_\Psi$ | 2 | $G^1_\Psi$ | 1 |
| (IV) | $y$ odd and $r = 5$ | $F^1_\Psi$ | 2 | $G^2_\Psi$ | $2^3$ |
| (V) | $y$ odd and $r = 4$ | $F^1_\Psi$ | 1 | $G^2_\Psi$ | $2^3$ |
| (VI) | $y$ odd and $r = 3$ | $F^1_\Psi$ | $2^3$ | $G^2_\Psi$ | $2^5$ |
| (VII) | $y \equiv \beta \pmod 4$ and $r = 2$ | $F^1_\Psi$ | $2^3$ | $G^2_\Psi$ | $2^2$ |
| (VIII) | $y \equiv -\beta \pmod 4$ and $r = 2$ | $F^1_\Psi$ | $2^3$ | $G^3_\Psi$ | $2^3$ |
| (IX) | $y$ odd and $r = 1$ | $F^2_\Psi$ | $2^5$ | $G^4_\Psi$ | $2^7$ |

TABLE 2. Frey Curves of the H-Family, for $3 \mid \beta$

| Case | Conditions on $\beta$, $y$ | H-Frey curve | $L_3$ |
|---|---|---|---|
| (i) | $\mathrm{ord}_3(\beta) = 3$ | $H^1_\Psi$ | 1 |
| (ii) | $3 \mid y$ and $\mathrm{ord}_3(\beta) = 1,\ 2$ or $\mathrm{ord}_3(\beta) \geq 4$ | $H^1_\Psi$ | 3 |
| (iii) | $3 \nmid y$ and $\mathrm{ord}_3(\beta) = 2$ | $H^1_\Psi$ | $3^3$ |
| (iv) | $3 \nmid y$ and $\mathrm{ord}_3(\beta) = 1$ | $H^1_\Psi$ | $3^4$ |

TABLE 3. Frey Curves of the H-Family, for $3 \mid \alpha$

| Case | Conditions on $\alpha$, $x$ | H-Frey curve | $L_3$ |
|---|---|---|---|
| (i) | $\mathrm{ord}_3(\alpha) = 3$ | $H^2_\Psi$ | 1 |
| (ii) | $3 \mid y$ and $\mathrm{ord}_3(\beta) = 1,\ 2$ or $\mathrm{ord}_3(\alpha) \geq 4$ | $H^2_\Psi$ | 3 |
| (iii) | $3 \nmid y$ and $\mathrm{ord}_3(\alpha) = 2$ | $H^2_\Psi$ | $3^3$ |
| (iv) | $3 \nmid y$ and $\mathrm{ord}_3(\alpha) = 1$ | $H^2_\Psi$ | $3^4$ |

The 'H-family':

$$H^1_\Psi: \quad Y^2 + 3XY - \Psi Y = X^3, \qquad H^2_\Psi: \quad Y^2 + 3XY + (\Psi + 1)Y = X^3,$$
$$H^3_\Psi: \quad Y^2 - 3XY + \Psi Y = X^3.$$

Before giving our main Proposition on level-lowering we list some useful properties of these Frey curves.

**Lemma 3.1.**
- *All primes $l \neq 2$ are primes of moderate reduction for the surfaces in the F- and G-families. All primes $l \neq 3$ are primes of moderate reduction for the surfaces in the H-family.*
- *If $k$ is any field of characteristic $\neq 2$ then the fibers $F^i_\phi$ and $G^i_\phi$ are non-singular for all $\phi \in k \setminus \{-1, 0\}$ and nodal for $\phi = -1,\ 0$.*

TABLE 4. Frey Curves of the H-Family, for $3 \nmid \alpha,\ \beta$

| Case | Conditions on $\beta$, $x$, $y$ | H-Frey curve | $L_3$ |
|---|---|---|---|
| (i) | $3 \mid y$ | $H^1_\Psi$ | 3 |
| (ii) | $3 \mid x$ | $H^2_\Psi$ | 3 |
| (iii) | $3 \nmid xy$ and $2^r\beta y^p \equiv 8 \pmod 9$ | $H^1_\Psi$ | $3^2$ |
| (iv) | $3 \nmid xy$ and $2^r\beta y^p \equiv 2, 5 \pmod 9$ | $H^1_\Psi$ | $3^3$ |
| (v) | $3 \nmid xy$ and $2^r\beta y^p \equiv 4 \pmod 9$ | $H^3_\Psi$ | $3^2$ |
| (vi) | $3 \nmid xy$ and $2^r\beta y^p \equiv 1, 7 \pmod 9$ | $H^3_\Psi$ | $3^3$ |

- *If $k$ is any field of characteristic $\neq 3$ then the fibers $H^i_\phi$ are non-singular for all $\phi \in k \setminus \{-1, 0\}$ and nodal for $\phi = -1,\ 0$.*

*Proof.* The Lemma follows from a few simple computations. First we compute the resultants of $c_4$ and $\Delta$ and find these to be powers of 2 for members of the $F$- and $G$-families and powers of 3 for members of the $H$-family. The first part of the Lemma now follows from Lemma 2.3.

The discriminants of the generic fibers $F^i_\Psi$ and $G^i_\Psi$ are of the form

$$2^l \Psi^m (\Psi + 1)^n,$$

for some integers $l,\ m,\ n$ with $m,\ n > 0$. This shows that if $\phi \neq -1,\ 0$ and the characteristic is not 2, then $F^i_\phi$ and $G^i_\phi$ are non-singular. If $\phi = -1$ or 0 and the characteristic is not 2, then by the above $c_4 \neq 0$. Hence the fibers $F^i_\phi$ and $G^i_\phi$ are nodal. This proves the second part of the Lemma.

The third part follows similarly on observing that the discriminants for the generic fibers $H^i_\Psi$ are of the form

$$3^l \Psi^m (\Psi + 1)^n$$

for some integers $l,\ m,\ n$, with $m, n > 0$. □

If $R$ is a non-zero integer we denote by $\mathrm{Rad}(R)$ the product of the distinct primes dividing $R$. If $q$ is a prime, we denote by $\mathrm{Rad}_q(R)$ the product of distinct primes dividing $R$ and not equal to $q$.

**Proposition 3.2.** *Suppose $\alpha,\ \beta$ are integers satisfying conditions (6)–(7). Suppose $(p, r, x, y)$ is a solution to equation (5) satisfying conditions (8)–(11). Let $F_\Psi,\ G_\Psi,\ H_\Psi$ be respectively the $F$-, $G$-, $H$-Frey curves given by Tables 1–4. Let $L_1,\ L_2,\ L_3$ be also as given by these tables and let*

$$N_1 = L_1 \,\mathrm{Rad}(\alpha\beta), \qquad N_2 = L_2 \,\mathrm{Rad}(\alpha\beta), \qquad N_3 = L_3 \,\mathrm{Rad}_3\left(2^r \alpha\beta\right). \tag{12}$$

*Let $\psi = 2^r \beta y^p$. Then there exist newforms $f,\ g,\ h$ of levels $N_1,\ N_2,\ N_3$ respectively such that*

$$F_\psi \sim_p f, \qquad G_\psi \sim_p g, \qquad H_\psi \sim_p h. \tag{13}$$

*Remark.* In the light of the above proposition, it will be convenient to introduce the following terminology. If $\mathfrak{f} = (f, g, h)$ is a triple of newforms of levels $N_1,\ N_2,\ N_3$ as above, and $(p, r, x, y)$ is a solution to equation (5) satisfying all the foregoing conditions such that the relations (13) are satisfied with $\psi = 2^r \beta y^p$ then we say that the solution $(p, r, x, y)$ arises from the triple of newforms $\mathfrak{f}$ via the triple of Frey curves $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi, H_\Psi)$. Since there are only finitely many newforms at

any particular level, we see that there are only finitely many triples of newforms that can give rise to our solutions. For each such triple $\mathfrak{f}$ we can attempt to solve equation (5) under the assumption that the solution arises from the triple $\mathfrak{f}$. If we can do this for all possible triples $\mathfrak{f}$ we will have found all solutions to equation (5) satisfying conditions (8)–(11).

Often, it is simply more convenient to work with the pairs $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi)$ and $\mathfrak{f} = (f, g)$ and ignore the information Proposition 3.2 gives about the $H$-Frey curve.

*Proof of Proposition 3.2.* We note that equation (5) is a special case of equations $Ax^p + By^p + Cz^p = 0$, $Ax^p + By^p = Cz^2$ and $Ax^p + By^p = Cz^3$. Frey curves and level–lowering are detailed for these equations in respectively [19], [4], [5]. The Proposition is quite simply obtained by applying the recipes in those papers to this special case.

It is here that we make use of the condition (9), which is needed to ensure that the curves $F^i_\psi$, $G^i_\psi$ and $H^i_\psi$ are non-singular. The papers [4], [5] also add the condition that $xy \neq \pm 1$. This is needed in their context to ensure that the Frey curves do not have complex multiplication. In our setting we would like to ensure that the fibers $G^i_\psi$ and $H^i_\psi$ do not have complex multiplication. It turns out that condition (11), namely that $\psi = 2^r\beta y^p \neq \pm 2$, is sufficient to rule out complex multiplication. Indeed, a little computation shows that the $j$-invariants of the curves $G^i_\psi$, $H^i_\psi$ are never integral except possibly in the (excluded) case when $\psi = -2$. Let us give the details of this argument for $G^1_\psi$, the other cases being similar. A straightforward computation on a computer algebra system shows that the $j$-invariant of $G^1_\psi$ is

$$\frac{1728\psi^3 + 6912\psi^2 + 9216\psi + 4096}{\psi^3 + \psi^2}.$$

If this is integral, then the denominator $\psi^3 + \psi^2$ must divide the resultant of the numerator and denominator regarded as polynomials in $\psi$. This resultant is $2^{30}$. Since $\psi = 2^r\beta y^p$ is even by condition (10) we see that the only possible value for $\psi$ is $-2$ which we have excluded in our hypotheses.

Finally, for $p = 7$, we must ensure that the Galois representations on the 7-torsion of the curves $F^i_\psi$, $G^i_\psi$ and $H^i_\psi$ are irreducible [5, proof of Lemma 3.1]. Note that the $F^i_\psi$ and $G^i_\psi$ have points of order 2. If the Galois representation on the 7-torsion of one of them is reducible, then $F^i_\psi$ or $G^i_\psi$ corresponds to a non-cuspidal point on $X_0(14)$, and so is known to have $j$-invariant $j = -15^3$ or $255^3$. But this is impossible as we have already shown that the $j$-invariants of $F^i_\psi$ and $G^i_\psi$ are not integral. Thus the Galois representations on the 7-torsion of the curves $F^i_\psi$, $G^i_\psi$ are irreducible.

Suppose now that the Galois representation on the 7-torsion of the curve $H^i_\psi$ is reducible. As $H^i_\psi$ has the point $(0, 0)$ of order 3, the curve $H_i$ corresponds to a non-cuspidal point on $X_0(21)$, and so [5, proof of Lemma 3.1] has one of the following four $j$-invariants:

$$\frac{3^3 \cdot 5^3}{2}, \quad -\frac{3^2 \cdot 5^6}{2^3}, \quad -\frac{3^3 \cdot 5^3 \cdot 383^3}{2^7}, \quad \frac{3^2 \cdot 5^3 \cdot 101^3}{2^{21}}.$$

Equating the $j$-invariants of $H^i_\psi$ to these four values and solving gives us

$$\psi = 2, \quad -3, \quad \frac{3}{125}, \quad -\frac{128}{125}.$$

But $\psi = 2^r \beta y^p$ is integral and even, and so we see that $\psi = 2$ which we have excluded by our hypothesis (11). □

## 4. Bounding the Exponent $p$

Level-lowering often gives a way of bounding the exponent of a Diophantine equation. This idea is originally due to Serre [28, pages 203–204], and is now quite standard [4, Proposition 4.3], [10, Section 7], [29, Section 6]. In this section we give a diagonal version of Serre's idea, using two or three Frey curves simultaneously to maximize the chances of success. Our objective is to bound the exponent $p$ in equation (5), if possible. The following notation will greatly simplify later exposition. Suppose $S$ is a finite set of primes and let $E_\Psi$ be an $S$-integral elliptic surface, and $l \notin S$ a prime of moderate reduction for $E_\Psi$. Let $f$ be a newform with $q$-expansion as in (4) and coefficients $c_l$ generating the number field $K$. For $\phi \in \mathbb{F}_l$ let

$$D_l'(E_\phi, f) = \begin{cases} \mathrm{Norm}_{K/\mathbb{Q}}(a_l(E_\phi) - c_l), & \text{if } E_\phi \text{ is non-singular,} \\ \mathrm{Norm}_{K/\mathbb{Q}}\left((l+1)^2 - {c_l}^2\right), & \text{if } E_\phi \text{ is nodal,} \end{cases}$$

and

$$D_l(E_\phi, f) = \begin{cases} D_l'(E_\phi, f), & \text{if } K = \mathbb{Q}, \\ l \cdot D_l'(E_\phi, f), & \text{otherwise.} \end{cases}$$

If $\mathfrak{f} = (f_1, \ldots, f_n)$ is an $n$-tuple of newforms, $\mathfrak{E}_\Psi = (E_\Psi^{(1)}, \ldots, E_\Psi^{(n)})$ is an $n$-tuple of $S$-integral elliptic surfaces, and $l \notin S$ is a prime of moderate reduction for all of them then we let

$$B_{l,\phi}(\mathfrak{E}_\Psi, \mathfrak{f}) = \gcd\left\{ D_l(E_\phi^{(i)}, f_i) \quad : \quad i = 1, \ldots, n \right\},$$

and

$$B_l(\mathfrak{E}_\Psi, \mathfrak{f}) = \mathrm{lcm}\left\{ B_{l,\phi}(\mathfrak{E}_\Psi, \mathfrak{f}) \ : \quad \phi \in \mathbb{F}_l \right\}.$$

**Proposition 4.1.** *Let $\alpha$, $\beta$ be integers satisfying conditions* (6)-(7). *Suppose that $(p, r, x, y)$ is a solution to equation* (5) *satisfying conditions (8-11). Let $F_\Psi$, $G_\Psi$, $H_\Psi$ be the Frey curves and $L_1$, $L_2$, $L_3$ be the integers given by Tables 1–4. Let $N_1$, $N_2$, $N_3$ be given by* (12). *Suppose that $f$, $g$, $h$ are newforms of levels $N_1$, $N_2$, $N_3$ respectively giving rise to the solution $(p, r, x, y)$.*

(a) *If $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi)$, $\mathfrak{f} = (f, g)$ and $l \nmid 2\,\mathrm{Rad}(\alpha\beta)$ is prime then $p \mid B_l(\mathfrak{E}_\Psi, \mathfrak{f})$.*
(b) *If $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi, H_\Psi)$, $\mathfrak{f} = (f, g, h)$ and $l \nmid 6\,\mathrm{Rad}(\alpha\beta)$ is prime then $p$ divides $B_l(\mathfrak{E}_\Psi, \mathfrak{f})$.*

*Proof.* By definition of the phrase 'arises from' (see the remark after Proposition 3.2) we know that the relationships (13) hold with $\psi = 2^r \beta y^p$. Now suppose that $l \nmid 2\,\mathrm{Rad}(\alpha\beta)$. From Lemma 3.1, we know that $l$ is a prime of moderate reduction for $F_\Psi$ and $G_\Psi$. In particular, $l$ is a prime of good or nodal reduction for the fibers $F_\psi$ and $G_\psi$. Thus the models $F_\psi$, $G_\psi$ are minimal at $l$ and moreover have multiplicative reduction at $l$. It follows that $l^2$ does not divide the conductors of $F_\psi$, $G_\psi$. Neither does $l$ divide the levels $N_1$, $N_2$ of $f$ and $g$, since these are of the form $2^\epsilon\,\mathrm{Rad}(\alpha\beta)$ for some $\epsilon$. Let $\phi$ be the image of $\psi$ in $\mathbb{F}_l$. Applying Lemma 2.1 we see that

$$p \mid D_l(F_\phi, f), \qquad p \mid D_l(G_\phi, g).$$

Thus $p \mid B_{l,\phi}(\mathfrak{E}_\Psi, \mathfrak{f})$ with $\mathfrak{E}_\Psi = (E_\Psi, F_\Psi)$ and $\mathfrak{f} = (f, g)$. From the definition of $B_l(\mathfrak{E}_\Psi, f)$ we deduce that $p \mid B_l(\mathfrak{E}_\Psi, \mathfrak{f})$ as required. This proves (a). The proof of (b) is almost identical. □

The following is an immediate corollary to the above proof.

**Corollary 4.2.** *Suppose that the hypotheses of Proposition 4.1 are satisfied, in particular that the solution $(p, r, x, y)$ arises from $\mathfrak{f}$ via $\mathfrak{E}_\Psi$. Suppose that $l$ is a prime of moderate reduction for the surfaces in $\mathfrak{E}_\Psi$ that does not divide the levels of the newforms in $\mathfrak{f}$. Let*

$$\Phi_l = \{\phi \in \mathbb{F}_l \quad : \quad p \mid B_{l,\phi}(\mathfrak{E}_\Psi, \mathfrak{f})\}, \tag{14}$$

*As usual write $\psi = 2^r \beta y^p$. Then $\psi \equiv \phi \pmod{l}$ for some $\phi \in \Phi_l$.*

## 5. Some Remarks on the Multi-Frey Approach and on the Repeated Single-Frey Approach

Let us briefly explain the advantage of our multi-Frey approach over earlier approaches. Proposition 4.1 gives us an integer $B_l(\mathfrak{E}_\Psi, \mathfrak{f})$ and tells us that the exponent $p$ in our Diophantine equation (5) divides it. This information would of course be useless if $B_l(\mathfrak{E}_\Psi, \mathfrak{f}) = 0$. In such a case we have failed to bound the exponent $p$ using the prime $l$. If on the other hand $B_l(\mathfrak{E}_\Psi, \mathfrak{f}) \neq 0$ then we can list its prime factors and $p$ will be one of these; in this case we say that we have succeeded in bounding the exponent $p$ using the prime $l$.

With the single-Frey approach, we are computing $B_l(F_\Psi, f)$, $B_l(G_\Psi, g)$, $B_l(H_\Psi, h)$. Let us suppose for illustration that $f$ is a rational newform and so corresponds to an elliptic curve $F$. Now $B_l(F_\Psi, f) = 0$ if and only there is some value $\phi \in \mathbb{F}_l$ such that $F_\phi$ is non-singular and

$$a_l(F_\phi) = a_l(F).$$

Since $a_l(F_\phi)$ and $a_l(F)$ both belong to the interval $[-2\sqrt{l}, 2\sqrt{l}]$, it seems quite likely that this will be the case for some $\phi \in \mathbb{F}_l$.

In [3], Bennett uses what we call a repeated single-Frey approach. Essentially this means computing $B_l(F_\Psi, f)$, and if this is found to be 0, then computing $B_l(G_\Psi, g)$ and if this is found to be 0, then computing $B_l(H_\Psi, h)$. In the end we know that

$$p \mid \gcd\{B_l(F_\Psi, f), B_l(G_\Psi, g), B_l(H_\Psi, h)\}.$$

Let us now contrast with our method. Write $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi, H_\Psi)$. Suppose also for illustration that $f$, $g$, $h$ are rational newforms corresponding to elliptic curves $F$, $G$, $H$. Then $B_l(\mathfrak{E}_\Psi, \mathfrak{f}) = 0$ if and only if there is some $\phi \in \mathbb{F}_l$ such that $F_\phi$, $G_\phi$, $H_\phi$ are non-singular and

$$a_l(F_\phi) = a_l(F), \qquad a_l(G_\phi) = a_l(G), \qquad a_l(H_\phi) = a_l(H).$$

Notice that our method fails if there is some value $\phi \in \mathbb{F}_l$ such that there three equalities hold simultaneously. The repeated single-Frey fails if there are values $\phi_1$, $\phi_2$, $\phi_3 \in \mathbb{F}_l$ such that

$$a_l(F_{\phi_1}) = a_l(F), \qquad a_l(G_{\phi_2}) = a_l(G), \qquad a_l(H_{\phi_3}) = a_l(H).$$

It is evident that our approach is much more likely to succeed in obtaining a bound for $p$.

Let us now suppose that both methods succeed. Then both will give a list of possible values of the exponent $p$. The list of possible values given by our multi-Frey

method is very likely to be smaller than that given by the repeated single-Frey. In fact, $p$ appears in the list given by the repeated single-Frey if and only if there are values $\phi_1$, $\phi_2$, $\phi_3 \in \mathbb{F}_l$ such that

$$p \mid D_l(F_{\phi_1}, f), \qquad p \mid D_l(G_{\phi_2}, g), \qquad p \mid D_l(H_{\phi_3}, h).$$

By contrast, $p$ appears in the list given by the multi-Frey approach if and only if there is some $\phi \in \mathbb{F}_l$ such that

$$p \mid D_l(F_{\phi}, f), \qquad p \mid D_l(G_{\phi}, g), \qquad p \mid D_l(H_{\phi}, h).$$

It is evident that the list of possible values of the exponent $p$ given by the multi-Frey method is at least as small, and probably smaller, than that given by the repeated single-Frey.

## 6. First Examples

We would like to illustrate the use of Propositions 3.2 and 4.1 by using them to prove some special cases of Theorem 1. These examples have been chosen to also show the limitations of Proposition 4.1 and hence motivate the modular methods that we introduce later on.

For the examples below (and for the proofs of Theorems 1–3), we will need to explicitly compute all newforms at a given level. This can be done using the modular symbols algorithm [30], [12]. Thankfully, the modular symbols algorithm has been implemented as part of the computer algebra system `MAGMA` [7] by William Stein, and we use this whenever we need to compute newforms.

Apart from the computation of newforms, we need the following remarkable theorem of Bennett, mentioned previously in the introduction.

**Theorem 4.** *(Bennett [2]) Suppose $b$, $n$ are integers with $b \neq 0, -1$ and $n \geq 3$. Then the equation*

$$|(b+1)x^n - by^n| = 1$$

*has exactly one solution in positive integers $x$, $y$: namely $x = y = 1$.*

**Example 1.** For our first illustrative example we look at the equation

$$5^u x^p - 2^r y^p = 1, \qquad xy \neq 0, \quad 0 < u < p, \quad p \geq 7 \text{ is prime.}$$

We may suppose that $0 \leq r < p$. If $r > 0$ or $y$ is even then we take $\alpha = 5^u$ and $\beta = 1$. Otherwise rewrite the equation as $(-y)^p - 5^u(-x)^p = 1$ and take $\alpha = 1$ and $\beta = 5^u$. In either case we can apply Proposition 3.2 with $\mathrm{Rad}(\alpha\beta) = 5$, although we ignore the information this gives for the $H$-family. This is because we have found that ignoring the $H$-family reduces the number of cases to be considered, and is sufficient for our purpose.

Now Proposition 3.2 associates the putative solution to a pair of newforms $\mathfrak{f} = (f, g)$ of levels $N_1 = 5L_1$, $N_2 = 5L_2$ where $L_1$, $L_2$ are given by Table 1. We recall that there are no newforms at levels 5, 10. This shows that cases (I–V) of Table 1 are impossible. Let us look at case (VI). Here we know that the solution (if it exists) must arise from a pair of newforms $\mathfrak{f} = (f, g)$ via $\mathfrak{E} = (F^1_\Psi, G^2_\Psi)$, where $f$ has level 40 and $g$ has level 160. There is only one newform at level 40 which corresponds to the elliptic curve $40A1$ in Cremona's table; we write $f$ for this form. There are three newforms at level 160. The first two, call them $g_1$ and $g_2$, correspond to elliptic curves $160A1$ and $160B1$ respectively. The third is

$$g_3 = q + 2\sqrt{2}q^3 + q^5 - 2\sqrt{2}q^7 + \cdots .$$

Thus the solution (if it exists) must arise from one of the pairs $\mathfrak{f}_i = (f, g_i)$ ($i = 1, 2, 3$) via $\mathfrak{E} = (F^1_\Psi, G^2_\Psi)$. Now we compute

$$B_3(\mathfrak{E}_\Psi, \mathfrak{f}_1) = 0, \quad B_7(\mathfrak{E}_\Psi, \mathfrak{f}_1) = 24, \quad B_3(\mathfrak{E}_\Psi, \mathfrak{f}_2) = 4, \quad B_3(\mathfrak{E}_\Psi, \mathfrak{f}_3) = 48.$$

Proposition 4.1 asserts that if our solution arises from $\mathfrak{f}_i$ and if $l \nmid 10$ is prime then $p \mid B_l(\mathfrak{E}, \mathfrak{f}_i)$. Since $p \geq 7$ we see that there are no solutions satisfying the conditions of Case (VI). Notice that we had computed $B_3(\mathfrak{E}_\Psi, \mathfrak{f}_1)$ and found it to be zero, thus it gives no information about the prime $p$; this is not a problem here as $B_7(\mathfrak{E}_\Psi, \mathfrak{f}_1) = 24$. Cases (VIII) and (IX) were dealt with in a similar way to Case (VI).

Only Case (VII) remains; this corresponds to $r = 2$ and $y \equiv 1 \pmod 4$. Here Proposition 3.2 tells us that any solution must arise from a pair of newforms $\mathfrak{f} = (f, g)$ via $\mathfrak{E} = (F^1_\Psi, G^2_\Psi)$, where $f$ has level 40 and $g$ has level 20. Again $f$ corresponds to the elliptic curve $40A1$, and since there is exactly one newform at level 20, we see that $g$ corresponds to $20A1$. We now compute

$$B_3(\mathfrak{E}_\Psi, \mathfrak{f}) = 0, \quad B_7(\mathfrak{E}_\Psi, \mathfrak{f}) = 0, \quad B_{11}(\mathfrak{E}_\Psi, \mathfrak{f}) = 0, \quad B_{13}(\mathfrak{E}_\Psi, \mathfrak{f}) = 0, \ldots$$

and we are unable to bound $p$ using Proposition 4.1. In fact $B_l(\mathfrak{E}_\Psi, \mathfrak{f}) = 0$ for all primes $l \neq 2, 5$. To see this, note that the fibers $F^1_4$ and $G^2_4$ are isomorphic to $40A1$ and $20A1$ respectively. Thus if $l \neq 2, 5$ is prime, and $\phi = \overline{4} \in \mathbb{F}_l$ then

$$B_{l,\phi}(\mathfrak{E}, \mathfrak{f}) = \gcd\left\{a_l(F^1_\phi) - c_l, \quad a_l(G^2_\phi) - d_l\right\}$$

where $c_1$ and $d_l$ are respectively the $l$-th coefficients of $f$ and $g$. But $c_l = a_l(F^1_4) = a_l(F^1_\phi)$ and $d_l = a_l(G^2_4) = a_l(G^2_\phi)$. Thus $B_{l,\phi}(\mathfrak{E}, \mathfrak{f}) = 0$ and so $B_l(\mathfrak{E}, \mathfrak{f}) = 0$.

We should not be surprised that we fail to bound $p$ here since there is a solution that satisfies the conditions of Case (VII). Namely the solution $u = 1$, $r = 2$, $x = y = 1$ and $p$ arbitrary. We cannot prove that this is the only solution at this stage. We merely note that we have shown that it has $r = 2$, $y \equiv 1 \pmod 4$ and that the solution must arise from the pair $(40A1, 20A1)$ via $(F^1_\Psi, G^2_\Psi)$.

**Example 2.** We now turn our attention to the equation

$$3^u x^p - 2^r y^p = 1, \quad x, y \text{ non-zero integers}, \quad 0 < u < p. \tag{15}$$

We will solve this equation completely, though it will require more effort as, unlike Example 1, we need to use the $H$-family information.

Without loss of generality we assume that $0 \leq r < p$. First suppose that $r = 0$ and $y$ is odd. Then $x$ is even. Letting $\alpha = 1$ and $\beta = 3^u$ (and rewriting our equation as $(-y)^p - 3^u(-x)^p = 1$ we see that conditions (6)–(7) and (8)–(11) are satisfied. By Proposition 3.2, the solution arises from a pair of newforms at level 6. Since there are no newforms at level 6 we have a contradiction, and deduce that either $y$ is even or $r > 1$. Now we let $\alpha = 3^u$, $\beta = 1$. Again the conditions (6)–(7) and (8)–(11) are satisfied, unless $2^r \beta y^p = \pm 2$ which corresponds to the solution $(u, r, x, y) = (1, 1, -1, -1)$. So suppose that $(u, r, x, y) \neq (1, 1, -1, -1)$. Again we apply Proposition 3.2. We know that there are no newforms at levels 2, 3, 6, 12. Hence we deduce that we are in Cases (VI), (VIII), (IX) of Table 1 and Cases (iii), (iv) of Table 3.

Suppose that we are in Case (VI) of Table 1; this corresponds to the condition that $y$ is odd and $r = 3$. Then the solution arises from newforms at levels 24 and 96 via the Frey curves $F^1_\Psi$ and $G^2_\Psi$ respectively. There is only one newform $f$ at level 24; this corresponds to the elliptic curve $24A1$ in Cremona's tables. There are

TABLE 5. The triple of values $B_5(\mathfrak{E}_\Psi, \mathfrak{f})$, $B_7(\mathfrak{E}_\Psi, \mathfrak{f})$, $B_{11}(\mathfrak{E}_\Psi, \mathfrak{f})$ where $\mathfrak{f} = (f, g_i, h_j)$.

| | $h_1$ | $h_2$ | $h_3$ | $h_4$ |
|---|---|---|---|---|
| $g_1$ | 60, 336, 528 | 60, 84, 0 | 60, 84, 264 | 0, 336, 528 |
| $g_2$ | 60, 336, 0 | 60, 84, 264 | 60, 84, 264 | 0, 336, 0 |

two newforms $g_1$, $g_2$ at level 96; these correspond to elliptic curves $96A1$ and $96B1$ respectively. Now there are two possibilities for the corresponding '$H$-situation', namely Cases (iii) and (iv) of Table 3. Suppose that we are in Case (iv): that is $3 \nmid y$ and $u = 1$. Then our solution also arises from a newform at level 162 via $H^2_\Psi$. There are four newforms $h_1, \ldots, h_4$ at level 162, which correspond respectively to the elliptic curves $162A1$, $162B1$, $162C1$, $162D1$. Let $\mathfrak{E}_\Psi = (F^1_\Psi, G^2_\Psi, H^2_\Psi)$. According to Proposition 4.1, if the solution arises from the triple of newforms $\mathfrak{f} = (f, g_i, h_j)$ and $l \nmid 6$ is prime then $p \mid B_l(\mathfrak{E}_\Psi, \mathfrak{f})$. In Table 5 we give the values of of $B_l(\mathfrak{E}_\Psi, \mathfrak{f})$ for the primes $l = 5, 7, 11$.

Since $p \geq 7$ we immediately obtain a contradiction except when $\mathfrak{f} = (f, g_2, h_4)$. In that situation $p \mid 336 = 2^4 \times 3 \times 7$ and so it is possible that $p = 7$. However, we continue to compute (for $\mathfrak{f} = (f, g_2, h_4)$)

$$B_{13}(\mathfrak{E}_\Psi, \mathfrak{f}) = 0, \qquad B_{17}(\mathfrak{E}_\Psi, \mathfrak{f}) = 1224 = 2^3 \times 3^3 \times 17,$$

which gives a contradiction even for $p = 7$.

It follows that if we are in Case (VI) of Table 1 then we must be in Case (iii) of Table 3. In particular $r = 3$, $u = 2$ and equation (15) becomes

$$9x^p - 8y^p = 1.$$

This has the solution $(x, y) = (1, 1)$ and we know from Bennett's Theorem above that this must be the unique solution. Thus we have found all the solutions that correspond to Case (VI).

Similarly if we assume that we are simultaneously in Case (VIII) and Case (iii) we get a contradiction. Hence if we are in Case (VIII) then we must be in Case (iv) and then $r = 2$, $u = 1$ and we deduce that the only solution is $(x, y) = (-1, -1)$ as before.

Finally if we are in Case (IX) we also deduce quickly that $r = 1$, $u = 1$ and the only solution is $(1, 1)$. We summarize by saying that the only solutions to equation (15) are $(u, r, x, y) = (2, 3, 1, 1)$, $(1, 2, -1, -1)$, $(1, 1, 1, 1)$.

**Example 3.** Consider the equation

$$13^u x^p - 2^r y^p = 1, \quad x, y \text{ non-zero integers}, \quad 0 < u < p.$$

Again we may suppose that $0 \leq r < p$. If $r > 0$ or $y$ is even we choose $\alpha = 13^u$, $\beta = 1$. Otherwise let $\alpha = 1$, $\beta = 13^u$ (note that we can rewrite our equation as $(-y)^p - 13^u(-x)^p = 1$). In either case $\mathrm{Rad}(\alpha\beta) = 13$. We only consider Case (I) of Table 1; all other cases can be effortlessly eliminated as before. Apply Proposition 3.2; This tells us that the solution arises from a pair of newforms at level 26 via the pair of surfaces $\mathfrak{E}_\Psi = (F^1_\Psi, G^1_\Psi)$.

The newforms at level 26 are

$$f_1 = q - q^2 + q^3 + q^4 - 3q^5 - q^6 - q^7 + \cdots,$$
$$f_2 = q + q^2 - 3q^3 + q^4 - q^5 - 3q^6 + q^7 + \cdots.$$

These correspond respectively to the elliptic curves 26A1 and 26A2 in Cremona's tables [12]. Writing $\mathfrak{f} = (f_1, f_1)$, we easily compute $B_3(\mathfrak{E}_\Psi, \mathfrak{f}) = 15$. However Proposition 4.1 tells us that $p \mid B_3(\mathfrak{E}_\Psi, \mathfrak{f})$, contradicting our assumption that $p \geq 7$. We compute also $B_3(\mathfrak{E}_\Psi, \mathfrak{f}) = 1$ if $\mathfrak{f} = (f_1, f_2)$ and $B_3(\mathfrak{E}_\Psi, \mathfrak{f}) = 3$ if $\mathfrak{f} = (f_2, f_1)$, also giving contradictions. If $\mathfrak{f} = (f_2, f_2)$ then we find that

$$B_3(\mathfrak{E}_\Psi, \mathfrak{f}) = 7, \quad B_5(\mathfrak{E}_\Psi, \mathfrak{f}) = 5 \times 7, \quad B_7(\mathfrak{E}_\Psi, \mathfrak{f}) = 9 \times 7, \quad B_{11}(\mathfrak{E}_\Psi, \mathfrak{f}) = 60 \times 7, \ldots$$

which shows that $p = 7$ for any hypothetical solution to equation (23). It is instructive to see why $p = 7$ cannot be ruled out by Proposition 4.1. Suppose $l \nmid 26$ is prime. Let $\phi = \overline{0} \in \mathbb{F}_l$; from Lemma 3.1 we know that the fibers $F^1_\phi/\mathbb{F}_l$ and $G^1_\phi/\mathbb{F}_l$ are nodal. From the definition given in the previous section we see that $B_{l,\phi}(\mathfrak{E}_\Psi, \mathfrak{f}) = (l+1)^2 - c_l^2$ where $c_l$ is the $l$-th coefficient of $f_2$. By definition, $B_l(\mathfrak{E}_\Psi, \mathfrak{f})$ is divisible by $B_{l,\phi}(\mathfrak{E}_\Psi, \mathfrak{f})$ which in turn is divisible by $l + 1 - c_l = \sharp E(\mathbb{F}_l)$, where $E$ is the elliptic curve 26A2. According to [12] the curve $E$ has a point of order 7. It follows that $7 \mid B_l(\mathfrak{E}_\Psi, \mathfrak{f})$ for all primes $l \nmid 26$ and thus $p = 7$ cannot be ruled out using Proposition 4.1. It turns out that even when we use the $H$-family information, we cannot rule out $p = 7$ for a similar reason. It is still possible to obtain a contradiction in the case $p = 7$. Thus suppose $p = 7$ and $(r, x, y)$ is a solution to the above equation that arises from $\mathfrak{f} = (f_2, f_2)$ via $\mathfrak{E}_\Psi = (F^1_\Psi, G^1_\Psi)$. Let $\psi = 2^r \beta y^p$. Then we know that $F^1_\psi \sim_7 E$. Notice that

$$l + 1 - a_l(E) \equiv 0 \pmod 7, \qquad a_l(F_\psi) \equiv a_l(E) \pmod 7$$

for all but finitely many primes $l$. Thus $\sharp F_\psi(\mathbb{F}_l) = l + 1 - a_l(F_\psi) \equiv 0 \pmod 7$ for all but finitely many primes $l$. By the Chebotarev Density Theorem, $F_\psi$ has a $\mathbb{Q}$-rational subgroup of order 7 (see [27, IV–6]). Since $F_\psi$ has full 2-torsion, this is known to be impossible and we have deduced a contradiction.

## 7. A Negative Result

In Example 3, we had some trouble eliminating the exponent $p = 7$ due to the existence of a rational newform $f$ at the level predicted by Proposition 3.2 and satisfying the congruence $l + 1 - c_l \equiv 0 \pmod 7$ for almost all primes $l$. The reader will also recall that this congruence, which was the source of trouble, paradoxically helped us to eliminate the exponent $p = 7$.

This difficulty is not confined to rational newforms. Fortunately a similar technique is available for non-rational newforms, but this technique needs extra care. The following Lemma presents such a technique.

**Lemma 7.1.** *Let $\alpha$, $\beta$ be integers satisfying conditions (6)–(7). Suppose that $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi)$ or $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi, H_\Psi)$ is a Frey pair or triple and $\mathfrak{f} = (f, g)$ or $\mathfrak{f} = (f, g, h)$ is a newform pair or triple having levels $N_1$, $N_2$ (and $N_3$) as in Proposition 3.2. Suppose that newform $f$ satisfies conditions (i) and (ii) of Proposition 2.2 for some prime ideal $\mathfrak{p}$ of $K$ above $p$, where $K$ is the field generated by the coefficients of $f$. Suppose $q$ is some prime satisfying the following three conditions.*

(a) $q \neq p$.

(b) *$q$ is a prime of moderate reduction for the surfaces in $\mathfrak{E}_\Psi$ that does not divide the levels of the newforms in $\mathfrak{f}$.*

(c) *The product*

$$((q+1)^2 - c_q^2) \prod_{\phi \in \Phi_q \setminus \{\overline{-1}, \overline{0}\}} (a_q(F_\phi) - c_q) \tag{16}$$

*is not divisible by any prime ideal $\mathfrak{p}' \mid p$ of $K$ satisfying $\mathfrak{p}' \neq \mathfrak{p}$. Here $\Phi_q$ is given by* (14).

*Then there is no solution to equation* (5) *satisfying conditions* (8)–(11) *that arises from $\mathfrak{f}$ via $\mathfrak{E}_\Psi$.*

*Proof.* Suppose that there is some solution $(p, r, x, y)$ to equation (5) satisfying conditions (8)–(11) that arises from $\mathfrak{f}$ via $\mathfrak{E}_\Psi$. Letting $\psi = 2^r \beta y^p$ we see that $\mathfrak{E}_\psi \sim_p \mathfrak{f}$. In particular $F_\psi \sim_p f$. Thus there is some prime $\mathfrak{p}' \mid p$ of $K$ such that for all primes $l$

- if $l \nmid pN$ and $\psi \not\equiv -1, 0 \pmod{l}$ then $a_l(F_\psi) \equiv c_l \pmod{\mathfrak{p}'}$,
- if $l \nmid pN$ but $\psi \equiv -1$ or $0 \pmod{l}$ then $\pm(l+1) \equiv c_l \pmod{\mathfrak{p}'}$.

Applying this with $q$ in place of $l$ we see that either $\psi \not\equiv -1, 0 \pmod{q}$ in which case $a_q(F_\psi) \equiv c_l \pmod{\mathfrak{p}'}$ or else $\pm(q+1) \equiv c_q \pmod{\mathfrak{p}'}$. However, by Corollary 4.2 we know that $\psi \equiv \phi \pmod{q}$ for some $\phi \in \Phi_q$. We deduce that $\mathfrak{p}'$ divides the product in (16). Thus $\mathfrak{p}' = \mathfrak{p}$.

Hence $a_l(F_\psi) \equiv c_l \pmod{\mathfrak{p}}$ for all but finitely many primes $l$. However, by the hypotheses of the Lemma, the newform $f$ satisfies conditions (i) and (ii) of Proposition 2.2, and must therefore satisfy the conclusion of that Proposition. In particular $l+1 \equiv c_l \pmod{\mathfrak{p}}$ for all but finitely many $l$. It follows that $p \mid \sharp F_\psi(\mathbb{F}_l) = l + 1 - a_l(F_\psi)$ for all but finitely many primes $l$. By [27, IV–6], the elliptic curve $F_\psi$ has a $\mathbb{Q}$-rational subgroup of order $p$. Since $F_\psi$ has full 2-torsion and $p \geq 7$, this is known to be impossible, and we have reached a contradiction. □

The above Lemma is inspired by examples of Kraus [19, pages 1155–1156]; in those examples the possibility that the two primes $\mathfrak{p}$ and $\mathfrak{p}'$ could be distinct is not emphasized, although a priori we see no reason for them to be equal.

## 8. Predicting Exponents of Constants I

In most cases, for equations of the form (1)–(3), Proposition 4.1 allows us to show that the exponent belongs to some finite, small set of possibilities. One may then attempt to solve all the Thue equations for these particular exponents. In practice it often turns out that there are too many Thue equations to consider and that the coefficients of these are too large to enable us to solve them. We now assume that $p \geq 7$ is fixed, and give a method for predicting the exponents of the constants $q_1$, $q_2$ etc. in equations (1)–(3). This method is a multi-Frey and a multi-dimensional version of the method appearing in [9, Section 9], [29, Section 8].

It is convenient to consider a more general equation than (1)–(3), namely

$$A_1^{u_1} \cdots A_s^{u_s} x^p - B_1^{v_1} \cdots B_t^{v_t} y^p = 1, \qquad x,\ y \text{ are non-zero integers.} \tag{17}$$

We impose the following restrictions

$$A_1, \dots, A_s, B_1, \dots, B_t \text{ are distinct primes,} \tag{18}$$

$$p \geq 7 \text{ is prime,} \tag{19}$$

$$\text{either } y \text{ is even, or } B_1 = 2, \text{ all other } A_i, B_i \text{ are odd} \tag{20}$$

$$0 < u_i < p, \qquad 0 < v_i < p, \tag{21}$$

$$B_1^{v_1} \dots B_t^{v_t} y^p \neq \pm 2. \tag{22}$$

We let $\alpha = A_1^{u_1} \cdots A_s^{u_s}$. If $B_1 = 2$ we let $r = v_1$ and $\beta = B_2^{v_2} \cdots B_t^{v_t}$. If $B_1 \neq 2$ (and so all of the $A_i$, $B_i$ are odd) we let $r = 0$ and $\beta = B_1^{v_1} \cdots B_t^{v_t}$. We see now that any solution to equation (17) gives a solution to equation (5) with conditions (6)–(7) and (8)–(11) satisfied, making all of the foregoing applicable. In (21) we have imposed that all the $u_i$, $v_i$ are non-zero. This may appear puzzling, but is needed so that the value of $\mathrm{Rad}(\alpha\beta)$ does not depend on $u_i$, $v_i$. Thus by imposing these restrictions we are able to apply Propositions 3.2 and 4.1 without knowing the precise values of the exponents $u_i$, $v_i$; as stated previously our objective in this section is to determine the exponents $u_i$, $v_i$ having fixed $p \geq 7$ at the outset.

Applying Proposition 3.2 shows that any solution arises from one of a set of newforms triples (or pairs) $\mathfrak{f}$ via a corresponding set of Frey surface triples (or pairs) $\mathfrak{E}_\Psi$. We now would like to solve this equation under the assumption that the solution arises from a fixed newform pair $\mathfrak{f} = (f, g)$ (or triple $\mathfrak{f} = (f, g, h)$) via the Frey surface pair $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi)$ (or triple $\mathfrak{E}_\Psi = (F_\Psi, G_\Psi, H_\Psi)$) where $F_\Psi$, $G_\Psi$ (and $H_\Psi$) belong respectively to the $F$-, $G$- (and $H$-)Family. To remind, in our context, the phrase 'arises from' means that if we write $\psi = B_1^{v_1} \dots B_t^{v_t} y^p$ for the putative solution of equation (17) then $F_\psi \sim_p f$ and $G_\psi \sim_p g$ (and $H_\psi \sim_p h$ where relevant).

Suppose $l \neq 2$, 3, and so it follows from Lemma 3.1 that $l$ is a prime of moderate reduction for the surfaces. Let $\Phi_l$ be as in (14). Corollary 4.2 tells us that, with $\psi$ as above, there is some $\phi \in \Phi_l$ such that $\psi \equiv \phi \pmod{l}$. In other words, for some $\phi \in \Phi_l$ we have

$$A_1^{u_1} \dots A_s^{u_s} x^p \equiv \phi + 1, \qquad B_1^{v_1} \dots B_t^{v_t} y^p \equiv \phi \pmod{l}.$$

We will now restrict our prime $l$ to be of the form $np+1$. The motivation for this is that, even though we do not know $x$ and $y$, we know that the residue classes of $x^p$ and $y^p$ modulo $l$ belong to relatively small subset of $\mathbb{F}_l$, namely the subset of $p$-th powers. Knowing this subset of $p$-th powers in $\mathbb{F}_l$, together with $\Phi_l$ and employing the discrete logarithm, is our strategy for deducing information about the $u_i$, $v_i$.

So suppose that $l = np + 1$ is some prime. Let $g \in \mathbb{F}_l^*$ be a primitive root. The discrete logarithm with respect to $g$ is the isomorphism $\mathbb{F}_l^* \to \mathbb{Z}/(l-1)$ mapping $g^r$ to the residue class of $r$ modulo $l-1$. Since $p \mid (l-1)$, the discrete logarithm can be composed with the natural map $\mathbb{Z}/(l-1) \to \mathbb{F}_p$ to yield a surjective homomorphism $L_{l,p,g} : \mathbb{F}_l^* \to \mathbb{F}_p$. To ease notation, write $L_l$ for $L_{l,p,g}$, although it is implicitly understood that this map depends on the choice of the primitive root $l$. Suppose moreover that $\overline{-1}$, $\overline{0} \notin \Phi_l$. Then we know from the above that for some $\phi \in \Phi_l$,

$$u_1 L_l(A_1) + \dots + u_s L_l(A_s) \equiv L_l(\phi+1), \quad v_1 L_l(B_1) + \dots + v_t L_l(B_t) \equiv L_l(\phi) \pmod{p},$$

provided of course that $l$ was chosen so as not to divide any of the integers $A_j$, $B_j$. Given sufficiently many primes satisfying all of the foregoing conditions, the

problem of determining the $u_j$, $v_j$ (which we recall are subject to (21)) reduces to linear algebra over $\mathbb{F}_p$.

In fact, it is now straightforward to deduce the following.

**Proposition 8.1.** *With notation as above, let $l_1, \dots l_k$ be primes satisfying the following conditions:*

- *For all $j$, $l_j \nmid 6A_1 \dots A_s B_1 \dots B_t$.*
- *For all $j$, the primes $l_j \equiv 1 \pmod{p}$.*
- *For all $j$, the residue classes $\overline{-1}$, $\overline{0} \notin \Phi_j$ (where we write $\Phi_j$ for $\Phi_{l_j}$).*

*Let*

$$\mathcal{L} = (L_1, \dots, L_k) : \mathbb{F}_{l_1} \times \cdots \times \mathbb{F}_{l_k} \to \mathbb{F}_p^k,$$

*where we write $L_j$ for $L_{l_j}$. Define the $s \times k$ matrix $\mathbf{A} = (L_j(A_i))$ and the $t \times k$ matrix $\mathbf{B} = (L_j(B_i))$. Suppose that $(u_1, \dots, u_s, v_1, \dots, v_t, x, y)$ is a solution to equation (17), satisfying restrictions (18)–(22), and arising form $\mathfrak{f}$ via $\mathfrak{E}_\Psi$ as above. Writing $\mathbf{u} = (u_1, \dots, u_s)$, $\mathbf{v} = (v_1, \dots, v_t)$ we have the simultaneous congruences*

$$\mathbf{uA} \equiv \mathcal{L}(\mathbf{c} + (1, \dots, 1)), \qquad \mathbf{vB} \equiv \mathcal{L}(\mathbf{c}) \pmod{p}$$

*for some $\mathbf{c} \in \prod \Phi_j$.*

*Proof.* The proof follows from the above, but let us just note that the condition $l_j \nmid 6A_1 \dots A_s B_1 \dots B_t$ simultaneously implies that $l_j$ are primes of moderate reduction for the surfaces in $\mathfrak{E}_\Psi$, and that they do not divide the levels of the forms in $\mathfrak{f}$. □

**Example 4.** Consider the equation

$$17^u x^p - 11^v y^p = 1, \qquad xy \neq 0, \quad 0 < u,\ v < p, \quad p \geq 7 \text{ is prime.}$$

We assume that $y$ is even; the case where $y$ is odd is similar. Then according to Proposition 3.2 any solution arises from a pair of newforms at level $374 = 2 \times 11 \times 17$ via the Frey pair $\mathfrak{E}_\Psi = (F_\Psi^1, G_\Psi^1)$. There are 5 newforms at level 374 and so 25 pairs of newforms. We had no trouble eliminating 24 of these pairs using Proposition 4.1. The only troublesome pair is $\mathfrak{f} = (f, f)$ where

$$f = q - q^2 + \theta q^3 + q^4 + (\theta^2 - 4)q^5 - \theta q^6 + (-\theta^3 - 2\theta^2 + 7\theta + 10)q^7 + \cdots$$

with coefficients in $K = \mathbb{Q}(\theta)$ where $\theta^4 - \theta^3 - 10\theta^2 + 9\theta + 16 = 0$. We compute

$$B_3(\mathfrak{E}_\Psi, \mathfrak{f}) = 35280 = 2^4 \times 3^2 \times 5^1 \times 7^2,$$

thus we know by Proposition 4.1 that any solution must have $p = 7$. The trouble is that $B_l(\mathfrak{E}_\Psi, \mathfrak{f})$ is divisible by 7 for all $3 \leq l < 100$ with $l \nmid 374$. It seems that we are unable to eliminate $p = 7$ using Proposition 4.1. It also turns out that we are unable to rule out solutions with $p = 7$ using Lemma 7.1. So we use the method outlined above to eliminate $p = 7$. Let $l = 71$; we find that

$$\Phi_{71} = \left\{\overline{19},\ \overline{30},\ \overline{65}\right\} \subset \mathbb{F}_{71},$$

and so $l = 71$ satisfies the conditions of Proposition 8.1. Hence

$$17^u x^7 \equiv 20 \pmod{71}, \qquad 11^v y^7 \equiv 19 \pmod{71} \quad \text{or}$$
$$17^u x^7 \equiv 31 \pmod{71}, \qquad 11^v y^7 \equiv 30 \pmod{71} \quad \text{or}$$
$$17^u x^7 \equiv 66 \pmod{71}, \qquad 11^v y^7 \equiv 65 \pmod{71}.$$

Note that 7 is a primitive root of $\mathbb{F}_{71}$. Applying the map $L_{71,7,7}$ to the above we get

$$\begin{aligned} 0 &\equiv 5 \pmod 7, \qquad 3v \equiv 2 \pmod 7 \quad \text{or} \\ 0 &\equiv 4 \pmod 7, \qquad 3v \equiv 4 \pmod 7 \quad \text{or} \\ 0 &\equiv 0 \pmod 7, \qquad 3v \equiv 4 \pmod 7. \end{aligned}$$

Here we are helped with the fact that 17 is a 7-th power modulo 71 and so $L_{71,7,7}(17) = 0$. The first two possibilities above are impossible. Hence $v \equiv 6 \pmod 7$. Now we take $l = 127$. Then

$$\Phi_{127} = \left\{\overline{13},\ \overline{27},\ \overline{41},\ \overline{54},\ \overline{80},\ \overline{95},\ \overline{100},\ \overline{107}\right\} \subset \mathbb{F}_{127}.$$

Thus $11^v y^{17} \equiv \phi \pmod{127}$ for some $\phi \in \Phi_{127}$. This implies that $v \equiv 0,\ 1,\ 2,\ 5 \pmod 7$, contradicting the fact that $v \equiv 6 \pmod 7$ proved above. Hence there is no solution for $p = 7$, or indeed for any larger prime exponent.

*Remark.* With regard to Example 4, the referee remarked to us that equations of the form

$$Ax^p - By^p = 1$$

with $AB$ odd are most easily dealt with using the '$H$-family' of Frey curves. To see this, suppose $H_\Psi \sim_p h$ for some newform $h$. Clearly $2 \mid xy$ and it follows that $H_\Psi$ has nodal reduction at 2. By Lemma 2.1

$$p \mid \mathrm{Norm}_{K/\mathbb{Q}}(c_2^2 - 3^2),$$

where $c_2$ is the coefficient of $q^2$ in the $q$-expansion of $h$, and $K$ is the field of definition of the coefficients of $f$. The point is that this expression cannot be zero, since any conjugate $c$ of $c_2$ satisfies $|c| \le 2\sqrt{2} < 3$. Thus this approach will always yield a bound for $p$.

However, for Example 4, this does not help in eliminating the troublesome $p = 7$ case. To see this note that for Example 4, we have $H_\Psi \sim_p h$ where $h$ has level $3^i \times 11 \times 17$ and $i = 1,\ 2$ or 3. Now at level $3 \times 11 \times 17 = 561$ we have—among many others—the newform

$$h = q + \sqrt{2}q^2 + q^3 + (-\sqrt{2} - 2)q^5 + \sqrt{2}q^6 - 3q^7 \cdots .$$

We see that $p$ divides $\mathrm{Norm}(\sqrt{2}^2 - 3^2) = 49$, and so we have not eliminated $p = 7$.

## 9. Proof of Theorem 2

We programmed the methods outlined so far in `MAGMA`. These are powerful enough to prove Theorems 1–3 apart from a few cases.

*Proof of Theorem 2.* Our programs prove Theorem 2 completely. First we solve the relevant Thue equations (2) with exponents $n = 3,\ 4,\ 5$ using inbuilt `MAGMA` functions. Hence we can reduce to the equation

$$q_1^u x^p - q_2^v y^p = 1, \qquad xy \neq 0, \quad 0 \le u,\ v < p, \quad p \ge 7 \text{ is prime.}$$

We apply Proposition 3.2, but at first ignore the information for the $H$-family. We consider separately the three cases

- $u = 0$, $v > 0$; solutions here correspond to a pair of newforms of level $2q_2$.
- $u > 0$, $v = 0$; solutions here correspond to a pair of newforms of level $2q_1$.
- $u,\ v > 0$; solutions here correspond to a pair of newforms of level $2q_1q_2$.

Suppose first that $(q_1, q_2) \neq (19, 3)$. For each possible pair of newforms we were able to bound the exponent $p$ using Proposition 4.1. Indeed, for most pairs of newforms encountered, Proposition 4.1 completely eliminated all possible exponents $p \geq 7$. In all the other cases the remaining exponents were eliminated using Lemma 7.1 or Proposition 8.1.

The reason for supposing that $(q_1, q_2) \neq (19, 3)$ is that Proposition 4.1 failed to bound the exponent $p$ for this case using just the $F$ and $G$-information. Here we were forced to apply the full information given by Proposition 3.2 and then Proposition 4.1 eliminated all the exponents $p \geq 7$. This completes the proof. □

## 10. Substantial Subcases of Theorems 1, 3

Unfortunately we cannot completely prove Theorems 1, 3 using the methods explained so far. The reason is that Proposition 4.1 works by bounding the exponent. Occasionally the equation considered has solutions for all possible exponents, and Proposition 4.1 will fail to bound the exponent. However applying our `MAGMA` programs used above to prove Theorem 2 yields partial results in the directions of Theorems 1, 3. In this section we continue to use Cremona's code for elliptic curves as in either his book [12], or his extended online tables [13].

**Proposition 10.1.** *Suppose $p$, $q$ are primes with $p \geq 7$ and $3 \leq q < 100$. Then the equation*

$$q^u x^p - 2^r y^p = 1, \quad x, y \text{ non-zero integers}, \quad 0 \leq u, r < p, \tag{23}$$

*has no solutions unless*

(a) $(u, r, x, y) = (0, 1, -1, -1)$ *and $p$ is arbitrary.*
(b) $q = 3$ *and* $(u, r, x, y) = (1, 1, 1, 1), (1, 2, -1, -1), (2, 3, 1, 1)$ *and $p$ is arbitrary.*
(c) $q = 5$, $r = 2$ *and the solution arises from the pair* $(40A1, 20A1)$ *via* $(F_\Psi^1, G_\Psi^2)$.
(d) $q = 7$, $r = 3$ *and the solution arises from the pair* $(56A1, 224A1)$ *via* $(F_\Psi^1, G_\Psi^2)$.
(e) $q = 17$, $r = 4$ *and the solution arises from the pair* $(17A1, 136A1)$ *via* $(F_\Psi^1, G_\Psi^2)$.
(f) $q = 31$, $r = 5$ *and the solution arises from the pair* $(62A1, 248B1)$ *via* $(F_\Psi^1, G_\Psi^2)$.

*Remark.* Notice that in cases (c)-(f) we have not yet solved the equation (23) completely. A complete solution will essentially be the proof of Theorem 1.

*Proof.* Suppose first the $u = 0$. Then the equation is a special case of the equation $x^p + 2^r y^p + z^p = 0$ which has been solved by Wiles [33] for $r = 0$, Ribet [26] for $r > 1$ and Darmon and Merel [14] for $r = 1$. The only solution to this equation is $r = 1$ and $(x, y, z) = \pm(1, -1, 1)$. This gives (a). From now on we suppose that $u > 0$.

The cases with $q = 5$, 3, 13 are handled in Examples 1, 2, 3 respectively. The other cases are similar to these, except that Lemma 7.1 and Proposition 8.1 are occasionally needed to eliminate some possibilities. □

**Proposition 10.2.** *Suppose $p$ is a prime with $p \geq 7$. Then the equation*

$$5^u x^p - 2^r 3^s y^p = 1, \quad x, y \text{ non-zero integers}, \quad u, s > 0, \tag{24}$$

*has no solutions unless*

(a) $(r,s)=(4,1)$ *and the solution arises from the triple* $(15A1, 120B1, 810F1)$ *via* $(F_\Psi^1, G_\Psi^2, H_\Psi^1)$.
(b) $(r,s)=(3,1)$ *and the solution arises from the triple* $(120A1, 480C1, 810F1)$ *via* $(F_\Psi^1, G_\Psi^2, H_\Psi^1)$.
(c) $(r,s)=(1,1)$ *and the solution arises from the triple* $(480B1, 1920R1, 810E1)$ *or the triple* $(480G1, 1920M1, 810A1)$ *via* $(F_\Psi^2, G_\Psi^4, H_\Psi^1)$.
(d) $(r,s)=(1,2)$ *and the solution arises from the triple* $(480F1, 1920Q1, 270A1)$ *or the triple* $(480H1, 1920A1, 270C1)$ *via* $(F_\Psi^2, G_\Psi^4, H_\Psi^1)$.

*Proof.* The proof uses Proposition 3.2 and Proposition 4.1. For the proof we used the full $F$-, $G$- and $H$-information given by Proposition 4.1. The $F$- and $G$-information allows us to predict the exponent $r$, whilst the $H$-information allows us to predict the exponent $s$. This is very similar to Example 2 and we omit the details except for one comment: we are not surprised to find the pairs $(r,s)=(3,1)$ and $(r,s)=(1,1)$ since these correspond respectively to the solutions $(p,u,r,s,x,y)=(p,2,3,1,1,1)$ and $(p,u,r,s,x,y)=(p,1,1,1,-1,-1)$. We are however surprised at first sight to find the pairs $(r,s)=(4,1)$ and $(r,s)=(1,2)$, since the corresponding equations

$$5^u x^p - 48y^p = 1, \qquad 5^u x^p - 18y^p = 1$$

appear not to have solutions. Notice however that the equations

$$15x^p - 16y^p = 1, \qquad 10x^p - 9y^p = 1$$

do have obvious solutions, and these equations have the same powers of 2 and 3 appearing in the coefficients as in the previous equations. It is a limitation of the method of Proposition 4.1 that it does not distinguish between these two pairs of equations. □

Similarly we have the following result which also follows from Propositions 3.2 and 4.1

**Proposition 10.3.** *Suppose $p$ is a prime with $p \geq 7$. Then the equation*

$$7^u x^p - 2^r 3^s y^p = 1, \quad x,\ y \text{ non-zero integers}, \quad u,\ s > 0, \tag{25}$$

*has no solutions unless*

(a) $(r,s)=(6,2)$ *and the solution arises from the triple* $(42A1, 21A1, 378E1)$ *via* $(F_\Psi^1, G_\Psi^1, H_\Psi^1)$.
(b) $(r,s)=(4,1)$ *and the solution arises from the triple* $(21A1, 168A1, 1134F1)$ *via* $(F_\Psi^1, G_\Psi^2, H_\Psi^1)$.
(c) $(r,s)=(1,1)$ *and the solution arises from the triple* $(672E1, 2688C1, 1134H1)$ *or the triple* $(672F1, 2688T1, 1134D1)$ *via* $(F_\Psi^2, G_\Psi^4, H_\Psi^1)$.

## 11. Predicting Exponents of Constants II

In Proposition 10.1 we reduced equation (23) with $3 \leq q < 100$ prime to a few cases where the exponent $r$ is known. In other words, we reduced to an equation of the form

$$A'A^u x^p - By^p = 1, \qquad x,\ y,\ u \text{ are non-zero integers}, \ 0 < u < p, \tag{26}$$

where $A'$, $A$, $B$ are non-zero integers, with $A \geq 5$. We now give a result which enables us to predict the exponent $u$ and complete the resolution of such equations

using Bennett's Theorem (Theorem 4). The method here is motivated to some extent by [9, Lemma 7.4].

If $l$ is a prime $n$ a positive integer, we write

$$\mu_n(\mathbb{F}_l) = \{\zeta \in \mathbb{F}_l^* \ : \quad \zeta^n = 1\}. \tag{27}$$

**Proposition 11.1.** *Let $p \geq 7$ be a (fixed) prime. Suppose $A'$, $A$, $B$, $u_0$ are non-zero integers, with $B$ even, $A \geq 5$ and $0 < u_0 < p$. Suppose moreover that*

$$A'A^{u_0} - B = 1.$$

*Suppose that the solution $(u, x, y)$ to equation (26) arises from a pair of elliptic curves $(F, G)$ via the Frey pair $(F_\Psi, G_\Psi)$ where $F_\Psi$, $G_\Psi$ belong respectively to the $F$- and $G$-families. Suppose further that there is a positive integer $n$ satisfying the following conditions:*

(i) *The integer $l = np + 1$ is prime,*
(ii) $l \nmid 2A'AB$,
(iii) $A^n \not\equiv 1 \pmod{l}$,
(iv) $p \nmid (l + 1 \pm a_l(F))$ *or* $p \nmid (l + 1 \pm a_l(G))$,
(v) *for all $\zeta \in \mu_n(\mathbb{F}_l) \setminus \{\overline{1}\}$ with $B\zeta \not\equiv -1 \pmod{l}$,*

$$a_l(F_{B\zeta}) \not\equiv a_l(F) \pmod{p} \quad \text{or} \quad a_l(G_{B\zeta}) \not\equiv a_l(G) \pmod{p}.$$

*Then $(x, y, u) = (1, 1, u_0)$. Moreover, if $F$, $G$ have non-trivial 2-torsion and $l < p^2/4$ then we still obtain the same conclusion when we replace condition (v) by the following weaker condition:*

(v′) *for all $\zeta \in \mu_n(\mathbb{F}_l) \setminus \{1\}$ with $B\zeta \not\equiv -1 \pmod{l}$,*

$$a_l(F_{B\zeta}) \neq a_l(F) \quad \text{or} \quad a_l(G_{B\zeta}) \neq a_l(G).$$

*Proof.* We assume that (i)–(v) hold. Let $\psi = By^p$. If $By^p = 0, -2$ then $A'A^u x^p = \pm 1$ contradicting the fact that $A \geq 5$ and $u > 0$. Thus $\psi = By^p \neq 0, -2$.

By definition, since $(u, x, y)$ arises from $(F, G)$ via $(F_\Psi, G_\Psi)$ we see that $F_\psi \sim_p F$ and $G_\Psi \sim_p G$. Clearly $l \neq 2$ and so, by Lemma 3.1, is a prime of moderate reduction for $F_\Psi$, $G_\Psi$. Moreover from assumption (iv) and Lemma 2.1 we see that $l$ is a prime of good reduction for the curves $F_\psi$, $G_\psi$. But the discriminants of $F_\psi$, $G_\psi$ are of the form $\pm 2^\alpha (A'Ax^p)^\beta (By^p)^\gamma$ where $\beta$, $\gamma > 0$. Therefore $l \nmid x$, $y$. Again by Lemma 2.1

$$a_l(F_\psi) \equiv a_l(F) \pmod{p} \quad \text{and} \quad a_l(G_\psi) \equiv a_l(G) \pmod{p}.$$

But $\overline{y}^p \in \mu_n(\mathbb{F}_l)$ and so $\psi \equiv B\zeta$ for some $\zeta \in \mu_n(\mathbb{F}_l)$. By condition (v) we deduce that either $y^p \equiv 1 \pmod{l}$ or $By^p \equiv -1 \pmod{l}$. The latter is impossible since it implies that $l \mid A'Ax^p$, and hence the former congruence must hold. Thus

$$A'A^u x^p = By^p + 1 \equiv B + 1 \equiv A'A^{u_0} \pmod{l}.$$

Since $x^{np} = x^{l-1} \equiv 1 \pmod{p}$, we see that $A^{n(u-u_0)} \equiv 1 \pmod{l}$. However by (iii) we know that $A^n \not\equiv 1 \pmod{l}$. Since $l - 1 = np$ we deduce that $p \mid (u - u_0)$. But $0 < u_0,\ u < p$. Thus $u = u_0$. We have therefore reduced to the equation

$$A'A^{u_0} x^p - By^p = 1,$$

which now has fixed coefficients. By the hypotheses of the proposition, this has a solution $(x, y) = (1, 1)$. It follows from Bennett's Theorem (Theorem 4) that there can be no other solution. This completes the proof provided (i)–(v) hold.

The last part of the Proposition follows easily from Lemma 11.2 below. □

**Lemma 11.2.** *Suppose $E$ and $E'$ are two elliptic curves with non-trivial 2-torsion. Suppose $p$ is an odd prime, and $l$ an odd prime of good reduction for the two curves that satisfies $l < p^2/4$. Then $a_l(E) \equiv a_l(E') \pmod p$ if and only if $a_l(E) = a_l(E')$.*

*Proof.* The 'if' direction is obvious; let us proof the 'only if' direction. So suppose that $a_l(E) \equiv a_l(E') \pmod p$. Since $E$ and $E'$ have non-trivial 2-torsion we see that $a_l(E) = 2b$ and $a_l(E') = 2b'$ for some integers $b$, $b'$. Thus $b \equiv b' \pmod p$ and the Hasse–Weil bounds imply that $|b|$, $|b'| < \sqrt{l}$. Now the assumption $l < p^2/4$ forces $|b - b'| < p$ and hence $b = b'$. The Lemma follows. □

## 12. Proof of Theorem 1

We now complete the proof of Theorem 1.

*Proof of Theorem 1.* As in the proof of Theorem 2 we quickly reduce to the case where the exponent is a prime $p \geq 7$. We now apply Proposition 10.1. We see that we only have to resolve cases (c)–(f) of that Proposition. Indeed we have reduced to equations of the form

$$q^u x^p - By^p = 1 \tag{28}$$

where $(q, B) = (5, 4)$, $(7, 8)$, $(17, 16)$, $(31, 32)$. For pair $(q, B)$ we would like to show that the solution satisfying $|x| = |y|$ is unique. If however $|x|$, $|y| > 1$, then the method of [24] gives an upper bound for the exponent $p$ in (28). The bounds for the exponent $p$ are given in Table 6.

Table 6. Bounds on $p$ in equation (28), assuming that $|x|$, $|y| > 1$

| $(q, B)$ | bound on $p$ | $(q, B)$ | bound on $p$ |
|---|---|---|---|
| $(5, 4)$ | $48,679,097$ | $(7, 8)$ | $61,063,061$ |
| $(17, 16)$ | $102,981,207$ | $(31, 32)$ | $131,256,424$ |

We refer to [24] for the statement of the theoretical result we have applied. We only explain a small trick we used to obtain better bounds for $p$, when $(q, B) = (7, 8)$ or $(31, 32)$. To deal with (28), we introduce the linear form in three logarithms:

$$\Lambda = \log B - u \log q + p \log(y/x),$$

where $0 \leq u < p$. If $u > p/2$, then put $u_0 = u - p$, and otherwise set $u_0 = u$. We thus have

$$\Lambda = \log B - u_0 \log q + p \log\big(y/(qx)\big)$$

or

$$\Lambda = \log B - u_0 \log q + p \log(y/x).$$

Let $t$ be the integer such that $q^t \leq B < q^{t+1}$ and write

$$\Lambda = \log(Bq^{-t}) - (u_0 - t) \log q + p \log(yq^{-\epsilon}/x),$$

where $\epsilon = 0$ or 1. We then apply the theoretical result from [24] to the latter linear form in three logarithms. Our gain comes from the fact that $Bq^{-t}$ has the same height as $B$, but is much closer to 1 (when $t$ is positive).

We will explain how $(q, B) = (5, 4)$ is treated, the other cases are similar. Here we know from Proposition 10.1 that $r = 2$ and that the solution arises from the pair $(40A1, 20A1)$ via the Frey pair $(F^1_\Psi, G^2_\Psi)$. We also know that $u > 0$ from the

proof of Proposition 10.1. We note in passing that both curves $20A1$ and $40A1$ have non-trivial 2-torsion.

We now apply Proposition 11.1 with $A' = 1$, $A = 5$, $B = 4$, $u_0 = 1$, $E_\Psi = F_\Psi^1$ and $E = 40A1$. We wrote a `PARI/GP` [1] program which for each $7 \leq p \leq 2 \times 10^8$ searches for a corresponding $l$ satisfying conditions (i)–(iv), (v′) of Proposition 11.1. Our program succeeded in finding such an $l$ for all $p$ in the given range. The entire computation took about 25 hours on a dual processor AMD-Athlon MP 2200+ with clock speed 1800 MHz. Now Proposition 11.1 shows that $(u, x, y) = (1, 1, 1)$ is the unique solution for $7 \leq p \leq 2 \times 10^8$. In view of the bound on $p$ above, we see that our proof is complete for the case $(q, B) = (5, 4)$.

The proofs for the three other cases are similar; again we proved the uniqueness of the known solution for exponents $7 \leq p \leq 2 \times 10^8$ which in view of the above bounds is more than sufficient. The entire computer time for this proof (on the above mentioned machine) is about 100 hours. □

## 13. Eliminating Extraneous Triples

We are almost ready to prove Theorem 3, which we would like to deduce from Propositions 10.2 and 10.3. We can deal with cases (b), (c) of Proposition 10.2, and cases (b), (c) of Proposition 10.3 using Proposition 11.1. However, the cases (a), (d) of Proposition 10.2 and (a) of Proposition 10.3 appear extraneous; they do not seem to correspond to a solution. We would like to eliminate these cases. This we do using the following variant of Proposition 11.1.

**Proposition 13.1.** *Let $p \geq 7$ be a (fixed) prime. Suppose $A'$, $A$, $B$ are non-zero integers, with $B$ even, $A \geq 5$. Let $(F, G)$ be a pair of elliptic curves and $F_\Psi$, $G_\Psi$ belong respectively to the $F$- and $G$-families. Suppose further that there is a positive integer $n$ satisfying the following conditions:*

(i) *The integer $l = np + 1$ is prime,*
(ii) *$l \nmid 2A'AB$,*
(iii) *$A^n \not\equiv 1 \pmod{l}$,*
(iv) *$p \nmid (l + 1 \pm a_l(F))$ or $p \nmid (l + 1 \pm a_l(G))$,*
(v) *for all $\zeta \in \mu_n(\mathbb{F}_l)$ with $B\zeta \not\equiv -1 \pmod{l}$,*

$$a_l(F_{B\zeta}) \not\equiv a_l(F) \pmod{p} \quad \text{or} \quad a_l(G_{B\zeta}) \not\equiv a_l(G) \pmod{p}.$$

*Then equation (26) does not have any solution arising from the pair $(F, G)$ via $(F_\Psi, G_\Psi)$. Moreover, if $F$, $G$ have non-trivial 2-torsion and $l < p^2/4$ then we still obtain the same conclusion when we replace condition (v) by the following weaker condition:*

(v′) *for all $\zeta \in \mu_n(\mathbb{F}_l)$ with $B\zeta \not\equiv -1 \pmod{l}$,*

$$a_l(F_{B\zeta}) \neq a_l(F) \quad \text{or} \quad a_l(G_{B\zeta}) \neq a_l(G).$$

The proof of the above Proposition is similar to, but simpler than, the proof of Proposition 11.1.

## 14. Proof of Theorem 3

We now complete the proof of Theorem 3.

*Proof of Theorem 3.* As in the proof of Theorem 2 we quickly reduce to the case where the exponent is a prime $p \geq 7$. We now apply Propositions 10.2 and 10.3.

Thus we have a handful of equations of the form (28) where $(q, B) = (5, 48)$, $(5, 24)$, $(5, 6)$, $(5, 18)$, $(7, 576)$, $(7, 48)$, $(7, 6)$. Again, as in the proof of Theorem 1, assuming that $|x|$, $|y| > 1$, the method of [24] gives an upper bound for the exponent $p$ in (23). The bounds for the exponent $p$ are given in Table 7.

TABLE 7. Bounds on $p$ in equation (28), assuming that $|x|$, $|y| > 1$

| $(q, B)$ | $(5, 48)$ | $(5, 24)$ | $(5, 6)$ | $(5, 18)$ |
|---|---|---|---|---|
| bound on $p$ | $118,978,987$ | $167,798,750$ | $45,729,979$ | $142,006,412$ |
| $(q, B)$ | $(7, 576)$ | $(7, 48)$ | $(7, 6)$ | |
| bound on $p$ | $215,027,236$ | $261,178,348$ | $200,609,141$ | |

For the cases $(q, B) = (5, 24)$, $(5, 6)$, $(7, 48)$, $(7, 6)$, and for $p$ in the range $7 \leq p \leq 2 \times 10^8$ when $q = 5$ and $7 \leq p \leq 3 \times 10^8$ for $q = 7$, we showed that the obvious solutions are the unique ones using the `pari/gp` program based on Proposition 11.1. For the other extraneous cases, we used a program based on Proposition 13.1, which proved for $p$ in the above ranges that there are no solutions. The entire computations took around 310 hours on a dual processor AMD - Athlon MP 2200+ with clock speed of 1800 MHz. □

*Remark.* Baker's method for bounding the exponent $n$ for equation (3) involves a linear form in four logarithms. The best known bounds for linear forms in logarithms [22] will yield a bound for $n$ that is of the order $10^{20}$. Notice that using the modular approach we have predicted the exponents of 2 and 3 appearing in equation (3). Thus we have reduced to a linear form in three logarithms, and are able to get a bound of around $10^8$, by using [24]. The computations above would have been entirely unthinkable if the bound on the exponent is far greater than $10^{10}$.

This situation is reminiscent of the proof of the Fibonacci Powers Theorem [9] (the only perfect powers in the Fibonacci sequence are 0, 1, 8, 144). There, information obtained from the modular approach enables one to rewrite a linear form in three logarithms as a linear form in two logarithms. This leads to a reduction of the bound on the exponent from $2 \times 10^8$ (which in that context is a bound that is impossibly large), to 733 (which for the computation required is just about reasonable). This device, we believe, deserves further investigation.

## 15. Tables of Solutions

Table 8. Solutions to Equation (1) with $3 \leq q < 100$ and $x, y > 0$

| $q$ | $(u, r)$ | $n$ | $(x, y)$ |
|---|---|---|---|
| $q$ arbitrary | $(0, 1)$ | $n$ arbitrary | (1,1) |
| 3 | $(1, 1)$ | $n$ arbitrary | $(1, 1)$ |
| 3 | $(1, 2)$ | $n$ arbitrary | $(1, 1)$ |
| 3 | $(2, 3)$ | $n$ arbitrary | $(1, 1)$ |
| 3 | $(2, 0)$ | 3 | $(1, 2)$ |
| 5 | $(1, 2)$ | $n$ arbitrary | $(1, 1)$ |
| 5 | $(1, 0)$ | 4 | $(2, 3)$ |
| 7 | $(1, 3)$ | $n$ arbitrary | $(1, 1)$ |
| 7 | $(1, 0)$ | 3 | $(1, 2)$ |
| 17 | $(1, 4)$ | $n$ arbitrary | $(1, 1)$ |
| 17 | $(1, 0)$ | 3 | $(7, 18)$ |
| 17 | $(1, 1)$ | 3 | $(1, 2)$ |
| 17 | $(1, 0)$ | 4 | $(1, 2)$ |
| 19 | $(1, 0)$ | 3 | $(3, 8)$ |
| 31 | $(1, 5)$ | $n$ arbitrary | $(1, 1)$ |
| 31 | $(1, 2)$ | 3 | $(1, 2)$ |
| 31 | $(1, 1)$ | 4 | $(1, 2)$ |
| 31 | $(1, 0)$ | 5 | $(1, 2)$ |
| 37 | $(1, 0)$ | 3 | $(3, 10)$ |
| 43 | $(1, 0)$ | 3 | $(2, 7)$ |
| 53 | $(1, 1)$ | 3 | $(1, 3)$ |

TABLE 9. Solutions to Equation (2) with $3 \leq q_2 < q_1 \leq 31$ primes and $x,\, y > 0$

| $q_1,\quad q_2$ | $(u,r)$ | $n$ | $(x,y)$ |
|---|---|---|---|
| $5 \leq q_1 \leq 31,\quad q_2 = 3$ | $(0,2)$ | 3 | $(2,1)$ |
| $7 \leq q_1 \leq 31,\quad q_2 = 5$ | $(0,1)$ | 4 | $(3,2)$ |
| $q_1 = 5,\quad q_2 = 3$ | $(1,0)$ | 4 | $(2,3)$ |
| $11 \leq q_1 \leq 31,\quad q_2 = 7$ | $(0,1)$ | 3 | $(2,1)$ |
| $q_1 = 7,\quad q_2 = 3, 5$ | $(1,0)$ | 3 | $(1,2)$ |
| $19 \leq q_1 \leq 31,\quad q_2 = 17$ | $(0,1)$ | 3 | $(18,7)$ |
| $q_1 = 17,\quad 3 \leq q_2 \leq 13$ | $(1,0)$ | 3 | $(7,18)$ |
| $19 \leq q_1 \leq 31,\quad q_2 = 17$ | $(0,1)$ | 4 | $(2,1)$ |
| $q_1 = 17,\quad 3 \leq q_2 \leq 13$ | $(1,0)$ | 4 | $(1,2)$ |
| $23 \leq q_1 \leq 31,\quad q_2 = 19$ | $(0,1)$ | 3 | $(8,3)$ |
| $q_1 = 19,\quad 3 \leq q_2 \leq 17$ | $(1,0)$ | 3 | $(3,8)$ |
| $q_1 = 31,\quad 3 \leq q_2 \leq 29$ | $(1,0)$ | 5 | $(1,2)$ |
| $q_1 = 5,\quad q_2 = 3$ | $(2,1)$ | 3 | $(1,2)$ |
| $q_1 = 7,\quad q_2 = 3$ | $(2,1)$ | 4 | $(1,2)$ |
| $q_1 = 13,\quad q_2 = 5$ | $(1,1)$ | 3 | $(8,11)$ |
| $q_1 = 17,\quad q_2 = 3$ | $(2,2)$ | 5 | $(1,2)$ |
| $q_1 = 17,\quad q_2 = 5$ | $(1,1)$ | 3 | $(2,3)$ |
| $q_1 = 19,\quad q_2 = 11$ | $(1,1)$ | 3 | $(5,6)$ |
| $q_1 = 23,\quad q_2 = 3$ | $(1,1)$ | 3 | $(1,2)$ |

TABLE 10. Solutions to Equation (3) with $q = 5,\, 7$ and $x,\, y > 0$

| $q$ | $(u,r,s)$ | $n$ | $(x,y)$ |
|---|---|---|---|
| 5 | $(1,1,1)$ | $n$ arbitrary | $(1,1)$ |
| 5 | $(2,3,1)$ | $n$ arbitrary | $(1,1)$ |
| 7 | $(1,1,1)$ | $n$ arbitrary | $(1,1)$ |
| 7 | $(2,4,1)$ | $n$ arbitrary | $(1,1)$ |
| 7 | $(2,1,1)$ | 3 | $(1,2)$ |
| 7 | $(1,1,3)$ | 4 | $(5,3)$ |

## References


[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to* PARI-GP, version 2.1.1. (See also http://pari.math.u-bordeaux.fr/)

[2] M. A. Bennett, *Rational approximation to algebraic numbers of small height: The Diophantine equation* $|ax^n - by^n| = 1$, J. reine angew. Math. 535 (2001), 1–49.

[3] M. A. Bennett, *Products of consecutive integers*, Bull. London Math. Soc. **36** (2004), no. 5, 683–694.

[4] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[5] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine Equations of Signature* $(p, p, 3)$, Compositio Math. **140** (2004), no. 6, 1399–1416.

[6] Yu. Bilu, G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.

[7] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also http://www.maths.usyd.edu.au:8000/u/magma/)

[8] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, No.4 (2001), 843–939.

[9] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Mathematics (to appear).

[10] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell Equation*, Compositio Mathematica **142** (2006), 31–62.

[11] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[12] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.

[13] J. E. Cremona, *Elliptic curve data*, http://www.maths.nott.ac.uk/personal/jec/

[14] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[15] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. **144** (1996), no. 1, 137–166.

[16] G. Frey, *Links between stable elliptic curves and certain Diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), 1–40.

[17] G. Frey, *Links between solutions of* $A - B = C$ *and elliptic curves*, in: Number Theory, Ulm 1987, Proceedings, Lecture Notes in Math. **1380**, Springer-Verlag, New York, Berlin, Heidelberg, 1989, 31–62.

[18] C. Heuberger, *On general families of parametrized Thue equations*, Algebraic number theory and Diophantine analysis (Graz, 1998), 215–238, de Gruyter, Berlin, 2000.

[19] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.

[20] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Mathematics **7** (1998), No. 1, 1–13.

[21] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

[22] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. English transl. in Izv. Math. **64** (2000), 1217–1269.

[23] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[24] M. Mignotte, A kit on linear forms in 3 logarithms, to appear.

[25] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[26] K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. **LXXIX.1** (1997), 7–15.

[27] J.-P. Serre, *Abelian* $l$*-adic representations and elliptic curves*, W. A. Benjamin, 1968.

[28] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[29] S. Siksek, *The modular approach to Diophantine equations*, in *Explicit Methods in Number Theory*, to appear.

[30] W. A. Stein, *An introduction to computing modular forms using modular symbols*, in *Algorithmic Number Theory*, eds J. Buhler and P. Stevenhagen (Cambridge University Press, to appear).
[31] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
[32] E. Thomas, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory **34** (1990), 235–250.
[33] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Yann Bugeaud, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France
*E-mail address*: bugeaud@math.u-strasbg.fr

Maurice Mignotte, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France
*E-mail address*: mignotte@math.u-strasbg.fr

Samir Siksek, Institute of Mathematics, University of Warwick, Coventry, CV4 7AL, United Kingdom
*E-mail address*: siksek@maths.warwick.ac.uk