

## Perfect powers expressible as sums of two fifth or seventh powers

by

SANDER R. DAHMEN (Amsterdam) and SAMIR SIKSEK (Coventry)

**1. Introduction.** Let  $p, q, r \in \mathbb{Z}_{\geq 2}$ . The equation

$$(1.1) \quad x^p + y^q = z^r$$

is known as the generalized Fermat equation (or the Fermat–Catalan equation) with signature  $(p, q, r)$  (and unit coefficients). As in Fermat’s Last Theorem, one is interested in integer solutions  $x, y, z$ . Such a solution is called *non-trivial* if  $xyz \neq 0$ , and *primitive* if  $x, y, z$  are coprime. Let  $\chi = p^{-1} + q^{-1} + r^{-1}$ . The parametrization of non-trivial primitive integer solutions for  $(p, q, r)$  with  $\chi \geq 1$  has now been completed [12]. The Generalized Fermat Conjecture [9], [10] is concerned with the case  $\chi < 1$ . It states that the only non-trivial primitive integer solutions to (1.1) with  $\chi < 1$  are given by

$$\begin{aligned} 1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \\ 3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7, \\ 9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2, \\ 33^8 + 1549034^2 = 15613^3. \end{aligned}$$

The Generalized Fermat Conjecture has been established for many signatures  $(p, q, r)$ , including several infinite families of signatures. For exhaustive surveys see Cohen’s book [6, Chapter 14], or [1].

Many of the equations are solved using the modular approach to Diophantine equations. If we restrict ourselves to Frey curves over  $\mathbb{Q}$  and the signature  $(p, q, r)$  with  $\chi < 1$  consisting of only primes, then the only signatures (up to permutation) for which a Frey curve is known are given by

$$(l, l, l), (l, l, 2), (l, l, 3), (2, 3, l), (3, 3, l), (5, 5, l), (7, 7, l)$$

---

2010 *Mathematics Subject Classification*: Primary 11D41; Secondary 11F80, 11G30.

*Key words and phrases*: Chabauty–Coleman, curves, elliptic curves, Fermat–Catalan, Galois representations, generalized Fermat, Jacobians, modular forms.

where  $l$  is a prime ( $\geq 5, 5, 5, 7, 5, 2$  respectively to ensure that  $\chi < 1$ ). These Frey curves are all already mentioned in [9]. For all but the last two signatures, these Frey curves have been used to completely solve at least one Generalized Fermat equation (with unit coefficients, as always throughout this paper). In fact, the first three cases have completely been solved. The  $(l, l, l)$  case corresponds of course to Fermat's Last Theorem [28] (with exponent  $l \geq 5$ ), and the  $(l, l, 2)$  and  $(l, l, 3)$  cases have been solved for  $l \geq 7$  by Darmon and Merel [11] using a modular approach and for  $l = 5$  by Poonen [16] using descent on elliptic curves and Jacobians of genus 3 cyclic covers of the projective line. The  $(2, 3, l)$  case has only been solved (recall that we have now restricted ourselves to primes  $l \geq 7$ ) for  $l = 7$  using a combination of the modular approach and explicit methods (including Chabauty–Coleman) for determining  $\mathbb{Q}$ -rational points on certain genus 3 curves (twists of the Klein quartic); see [17]. Finally the  $(3, 3, l)$  case is solved for a set of prime exponents  $l$  with Dirichlet density  $\geq 0.628$ , and all  $l \leq 10^9$ ; see [5].

One feature that is common to the Frey curves associated to the first five signatures is that evaluating the Frey curve at a trivial solution gives either a singular curve, or an elliptic curve with complex multiplication. This is one of the main reasons why the first three signatures can be dealt with for all relevant prime exponents and why in the  $(3, 3, l)$  case so many prime exponents  $l$  can be handled. In the latter case the main obstruction to solving the equation completely is because of the Catalan solution (which is actually only present for  $l = 2$ , but nevertheless still forms an obstruction for larger primes  $l$ ). The Catalan solution also forms an obstruction for the  $(2, 3, l)$  case, but here there are many other difficulties.

The main reason why the Frey curves associated to signature  $(5, 5, l)$  or  $(7, 7, l)$  have not been used before to completely solve a generalized Fermat equation is probably that evaluating the Frey curve at a (primitive) trivial integer solution does not always give a singular or CM curve. In fact, only  $(\pm 1)^5 + (\mp 1)^5 = 0^l$  leads to a singular curve (throughout this paper, when  $\pm$  or  $\mp$  signs are present in a formula, they are meant to correspond in the obvious way within the formula). The modular approach however still gives a lot of non-trivial information. This allows us to combine the modular approach with the method of Chabauty–Coleman and descent techniques to solve three new cases of the generalized Fermat equations

$$(1.2) \quad x^5 + y^5 = z^l,$$

$$(1.3) \quad x^7 + y^7 = z^l.$$

In fact, the only values for which these equations have already been solved are covered by the first three families of exponent triples:  $(5, 5, 2)$  and  $(5, 5, 3)$  are solved by Poonen,  $(7, 7, 2)$  and  $(7, 7, 3)$  are solved by Darmon and Merel, while the cases  $(5, 5, 5)$  and  $(7, 7, 7)$  are of course special cases of Fermat's

Last Theorem, and the modular method using a Frey curve for exponent  $(l, l, l)$  works for these two special cases as well (of course there are classical descent proofs: exponent 5 was first solved around 1825 independently by Legendre and Dirichlet, exponent 7 was first solved around 1839 by Lamé). We see that the first two open cases for (1.2) and (1.3) are the signatures  $(5, 5, 7)$  and  $(7, 7, 5)$  respectively. In this paper we shall solve these equations, as well as the equation with signature  $(5, 5, 19)$ .

THEOREM 1. *Let  $l = 7$  or  $l = 19$ . Then the only solutions to the equation*

$$x^5 + y^5 = z^l$$

*in coprime integers  $x, y, z$  are  $(\pm 1, \mp 1, 0)$ ,  $(\pm 1, 0, \pm 1)$ , and  $(0, \pm 1, \pm 1)$ .*

THEOREM 2. *The only solutions to the equation*

$$(1.4) \quad x^7 + y^7 = z^5$$

*in coprime integers  $x, y, z$  are  $(\pm 1, \mp 1, 0)$ ,  $(\pm 1, 0, \pm 1)$ , and  $(0, \pm 1, \pm 1)$ .*

To prove Theorem 1, we exploit the fact that the associated Frey curve evaluated at a primitive trivial integer solution with  $z = 0$  gives a singular curve in order to solve (1.2) when  $5 \mid z$  for all primes  $l$ . For the remaining case  $5 \nmid z$ , we relate primitive integer solutions of (1.2) with  $l = 7$  and  $l = 19$  to  $\mathbb{Q}$ -rational points on a curve of genus 3 and 9 respectively, which we are able to determine using Chabauty–Coleman. For Theorem 2, we relate primitive integer solutions of (1.4) to  $K$ -rational points on genus 2 curves over the totally real cubic field  $K = \mathbb{Q}(\zeta + \zeta^{-1})$  where  $\zeta$  is a primitive 7th root of unity. Our factorization argument leads us in fact to 50 5-tuples of such genus 2 curves for which we need to determine the  $K$ -rational points for at least one curve per 5-tuple. We shall use the modular approach to rule out all but two of the 5-tuples of genus 2 curves. For the remaining two 5-tuples of curves, we were able to determine enough  $K$ -rational points using the method of Chabauty–Coleman to finish the proof of Theorem 2. We used the computer package MAGMA [2] for all our calculations. The MAGMA scripts we refer to in this paper are posted at [www.few.vu.nl/~sbn249/sumsofpowers.html](http://www.few.vu.nl/~sbn249/sumsofpowers.html).

Many of our computations depend on class group and unit group computations, which become significantly faster under assumption of the generalized Riemann hypothesis for Dedekind zeta functions (abbreviated as GRH from now on). As it turns out, assuming GRH, we can also deal with the exponents  $(5, 5, 11)$ ,  $(5, 5, 13)$ , and  $(7, 7, 11)$ .

THEOREM 3. *Assume GRH. If  $l \in \{11, 13\}$ , then (1.2) has no non-trivial primitive integer solutions. If  $l = 11$ , then (1.3) has no non-trivial primitive integer solutions.*

## 2. Preliminaries

**2.1. The method of Chabauty–Coleman.** Chabauty–Coleman is a method for bounding the number of  $K$ -rational points on a curve of genus  $\geq 2$  defined over a number field  $K$ , subject to certain conditions. We will need Chabauty–Coleman for the proof of our Theorems 1–3, and so we provide in this section a brief sketch of the method. For details we recommend the expository paper of McCallum and Poonen [15], as well as Wetherell’s thesis [27], and Coleman’s original paper [7].

Let  $C/K$  be a smooth projective geometrically integral curve of genus  $g \geq 2$ , and let  $J$  be its Jacobian. It is convenient to suppose the existence of  $K$ -rational points on  $C$  and fix one such point  $P_0 \in C(K)$ . We use  $P_0$  as the base for our Abel–Jacobi embedding:

$$j : C \rightarrow J, \quad P \mapsto [P - P_0].$$

Let  $\mathfrak{P}$  be a prime of good reduction for  $C$  and denote by  $K_{\mathfrak{P}}$  the  $\mathfrak{P}$ -adic completion of  $K$ . Write  $\Omega(C/K_{\mathfrak{P}})$  for the  $K_{\mathfrak{P}}$ -vector space of regular differentials on  $C$ , and  $\Omega(J/K_{\mathfrak{P}})$  for the corresponding space on  $J$ . Both these spaces have dimension  $g$ , and the Abel–Jacobi embedding induces an isomorphism  $j^* : \Omega(C/K_{\mathfrak{P}}) \rightarrow \Omega(J/K_{\mathfrak{P}})$ ; this is independent of the choice of the base point  $P_0$ , and we shall use it to identify the two spaces.

The method of Chabauty is based on the integration pairing

$$(2.1) \quad \Omega(C/K_{\mathfrak{P}}) \times J(K_{\mathfrak{P}}) \rightarrow K_{\mathfrak{P}}, \quad (\omega, D) \mapsto \int_0^D \omega.$$

The Mordell–Weil group  $J(K)$  is contained in  $J(K_{\mathfrak{P}})$ . Let  $r$  be its rank, and write  $\text{Ann}(J(K))$  for the  $K_{\mathfrak{P}}$ -subspace of  $\Omega(C/K_{\mathfrak{P}})$  that annihilates  $J(K)$  in the above pairing. If  $r < g$ , then it has dimension at least  $g - r$ . Suppose  $\text{Ann}(J(K))$  is positive-dimensional and let  $\omega$  be a non-zero differential belonging to it. Denote by  $\mathbb{F}_{\mathfrak{P}}$  the residue class field of  $K_{\mathfrak{P}}$ , let  $p$  be its characteristic and let  $e$  denote the absolute ramification index of  $\mathfrak{P}$ . We scale  $\omega$  so that it reduces to a non-zero differential  $\bar{\omega}$  on the reduction  $\tilde{C}/\mathbb{F}_{\mathfrak{P}}$ . The differential  $\omega$  can be used to bound the number of  $K$ -rational points  $C(K)$ . In particular, if  $\bar{\omega}$  does not vanish at  $\bar{P} \in \tilde{C}(\mathbb{F}_{\mathfrak{P}})$  and  $e < p - 1$ , then there is at most one  $K$ -rational point  $P$  on  $C$  that reduces to  $\bar{P}$  modulo  $\mathfrak{P}$ .

REMARK 2.1. In [21] a modified version of the above method is developed where instead of the traditional  $r \leq g - 1$  condition of Chabauty–Coleman the necessary condition of the new method is  $r \leq [K : \mathbb{Q}](g - 1)$ . However, as it turns out, the ‘classical’ Chabauty–Coleman method sketched above suffices for our purposes.

**2.2. The modular approach.** Our proofs will make heavy use of the modular approach to Diophantine equations, involving Frey curves, modularity, Galois representations and level-lowering. For an introduction, the reader can consult e.g. [6, Chapter 15] or [8, Chapter 2]. By a newform of level  $N$  we will mean a cuspidal newform of weight 2 with respect to  $\Gamma_0(N)$  (so the character is trivial). A newform is always normalized by default (i.e. the first Fourier coefficient of the expansion at the infinite cusp equals 1).

**2.3. A standard factorization lemma.** The following simple result will be very useful when we are factorizing  $x^5 + y^5$  and  $x^7 + y^7$ .

LEMMA 2.2. *Let  $p$  be an odd prime and  $x, y$  coprime integers. Write*

$$H_p = \frac{x^p + y^p}{x + y}.$$

*Then  $g := \gcd(x + y, H_p) = 1$  or  $p$ . Consequently,  $g = p \Leftrightarrow p \mid x^p + y^p \Leftrightarrow p \mid H_p \Leftrightarrow p \mid x + y$ . Moreover,  $p^2 \nmid H_p$ .*

*Proof.* Let  $u = -(x + y)$ . Then using the binomial formula we get

$$H_p = \frac{(y + u)^p - y^p}{u} = \sum_{k=1}^p \binom{p}{k} u^{k-1} y^{p-k}.$$

From the expression above we see that  $g \mid py^{p-1}$ . Since  $\gcd(u, y) = \gcd(x, y) = 1$ , we get  $g \mid p$ . Furthermore, if  $p \nmid u$ , then using  $p \mid \binom{p}{k}$  for  $k = 1, \dots, p - 1$  we see that  $p \nmid H_p$ . If  $p \mid u$ , then  $H_p \equiv py^{p-1} \pmod{p^2}$ , which is non-zero modulo  $p^2$  since  $p \nmid y$ . ■

**3. Proof of Theorem 1.** In light of Lemma 2.2 it is natural to distinguish two cases: non-trivial primitive integer solutions to (1.2) with  $5 \nmid z$  on the one hand, and those with  $5 \mid z$  on the other hand. For the former case, we relate non-trivial primitive integer solutions to (1.2) for some odd prime  $l$  to determining  $\mathbb{Q}$ -rational points on the hyperelliptic curve

$$(3.1) \quad C_l : Y^2 = 20X^l + 5.$$

Note that this curve has genus  $(l - 1)/2$  and that

$$C_l(\mathbb{Q}) \supset \{\infty, (1, \pm 5)\}.$$

LEMMA 3.1. *Let  $l$  be an odd prime. If*

$$(3.2) \quad C_l(\mathbb{Q}) = \{\infty, (1, \pm 5)\},$$

*then there are no non-trivial primitive integer solutions to (1.2) with  $5 \nmid z$ .*

*Proof.* Suppose that  $x, y, z$  are non-zero coprime integers satisfying (1.2). Then

$$(3.3) \quad (x + y)H_5 = z^l.$$

For any odd prime  $p$ , we see that  $H_p$  is a symmetric binary form of even degree in  $x, y$ , hence a binary form in  $x^2 + y^2$  and  $(x + y)^2$ . For  $p = 5$  we have explicitly

$$(3.4) \quad 5(x^2 + y^2)^2 = 4H_5 + (x + y)^4.$$

We assume  $5 \nmid z$ . By Lemma 2.2 we have  $\gcd(x + y, H_5) = 1$ . Hence (3.3) yields

$$(3.5) \quad x + y = z_1^l, \quad H_5 = z_2^l$$

where  $z_1, z_2$  are coprime non-zero integers satisfying  $z = z_1 z_2$ . Using identity (3.4) we have

$$5(x^2 + y^2)^2 = 4z_2^l + z_1^{4l}.$$

Multiplying both sides by  $5/z_1^{4l}$ , we see that

$$P := \left( \frac{z_2}{z_1^4}, \frac{5(x^2 + y^2)}{z_1^{2l}} \right) \in C_l(\mathbb{Q}).$$

Since  $z_1 \neq 0$ , we have  $P \neq \infty$ . If  $P = (1, \pm 5)$ , then we see that  $z_2 = 1$  and  $z_1 = \pm 1$ , which by (3.5) leads to  $xy = 0$ , a contradiction which proves the lemma. ■

We expect that (3.2) holds for all primes  $l \geq 7$  (it holds for  $l = 5$ , but we do not need this here). The cases we can prove at the present are summarized as follows.

PROPOSITION 3.2. *If  $l = 7$  or  $l = 19$ , then*

$$C_l(\mathbb{Q}) = \{\infty, (1, \pm 5)\}.$$

A proof, using 2-descent on hyperelliptic Jacobians and the method of Chabauty–Coleman, is given in Section 3.1 below. In a similar fashion we can reduce proving the non-existence of non-trivial primitive integer solutions with  $5 \mid z$  (to (1.2) for some odd prime  $l$ ) to finding  $\mathbb{Q}$ -rational points on a twist of  $C_l$ ; see Section 3.3. We can however deal with this case in a uniform manner for all primes  $l \geq 7$  using the modular method; see Section 3.2. Taking into account previously solved small exponent cases, we have in fact a complete solution in the  $5 \mid z$  case.

PROPOSITION 3.3. *Let  $l \geq 2$  be an integer. There are no non-trivial primitive integer solutions to (1.2) with  $5 \mid z$ .*

Trivially, Lemma 3.1 and Propositions 3.2 and 3.3 together imply Theorem 1.

**3.1. Rational points on  $C_l$ .** Let  $J_l$  denote the Jacobian of  $C_l$  and  $g_l = (l - 1)/2$  the genus of  $C_l$  (which equals the dimension of  $J_l$ ). In order to use Chabauty–Coleman to determine the  $\mathbb{Q}$ -rational points on  $C_l$  for some  $l$ ,

it is necessary that the Chabauty condition,  $\text{rank } J_l(\mathbb{Q}) < g_l$ , is satisfied and we need to compute a subgroup of finite index in the Mordell–Weil group  $J_l(\mathbb{Q})$ .

Before we go into the rank computations, we start with a description of the torsion subgroup  $J_l(\mathbb{Q})_{\text{tors}}$  of  $J_l(\mathbb{Q})$ . The curve  $C_l$ , and hence its Jacobian  $J_l$ , has good reduction away from 2, 5,  $l$ . For any odd prime  $p$  of good reduction, the natural map

$$J_l(\mathbb{Q})_{\text{tors}} \rightarrow J_l(\mathbb{F}_p)$$

is injective. In the rest of this section,  $l$  will always stand for a prime in the range  $7 \leq l \leq 19$ . Using **MAGMA** we find, for every prime  $l$  in our range, two primes  $p_1 \neq p_2$  distinct from 2, 5, or  $l$  such that

$$\gcd(\#J_l(\mathbb{F}_{p_1}), \#J_l(\mathbb{F}_{p_2})) = 1.$$

This shows that for all these primes  $l$  we have  $J_l(\mathbb{Q})_{\text{tors}} = \{0\}$ . To be concrete, for  $l = 7, 11, 13, 17, 19$  we can take  $(p_1, p_2) = (3, 43), (13, 23), (3, 53), (3, 103), (7, 191)$  respectively.

As for the rank computations, **MAGMA** includes implementations by Nils Bruin and Michael Stoll of 2-descent on Jacobians of hyperelliptic curves over number fields; the algorithm is detailed in Stoll’s paper [25]. Using this we were able to compute the 2-Selmer ranks of  $J_l/\mathbb{Q}$  for the primes  $l$  in our range (and no further, not even assuming GRH). The values are given in Table 1 below together with the time it took to compute them on a machine

**Table 1.** Rank bounds for the Jacobian of  $C_l$

$l$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(\mathbb{Q}, J_l)$	Time
7	1	0.4 s
11	2	3 s
13	2	23 s
17	2	4821 s $\approx$ 1.3 h
19	1	109819 s $\approx$ 30.5 h

with two Intel Xeon dual core CPUs at 3.0 GHz. We want to stress that the **MAGMA** routine `TwoSelmerGroup` involved makes use of the pseudo-random number generator of **MAGMA**. So the exact time also depends on the seed. From the usual exact sequence

$$0 \rightarrow J_l(\mathbb{Q})/2J_l(\mathbb{Q}) \rightarrow \text{Sel}^{(2)}(\mathbb{Q}, J_l) \rightarrow \text{III}(\mathbb{Q}, J_l)[2] \rightarrow 0$$

together with the fact that  $J_l(\mathbb{Q})$  has no 2-torsion, we get

$$(3.6) \quad \begin{aligned} \text{rank } J_l(\mathbb{Q}) &= \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(\mathbb{Q}, J_l) - \dim_{\mathbb{F}_2} \text{III}(\mathbb{Q}, J_l)[2] \\ &\leq \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(\mathbb{Q}, J_l). \end{aligned}$$

Let  $D = [(1, 5) - \infty]$ ; then  $D$  is a non-zero element of  $J_l(\mathbb{Q})$  and therefore (remembering that  $J_l(\mathbb{Q})_{\text{tors}} = \{0\}$ ) has infinite order. This shows that

$$\text{rank } J_l(\mathbb{Q}) \geq 1.$$

In particular, we deduce from the 2-Selmer ranks of  $J_l/\mathbb{Q}$  in Table 1 that for  $l = 7, 19$  we have  $\text{rank } J_l(\mathbb{Q}) = 1$  and  $D$  generates a subgroup of finite index in  $J_l(\mathbb{Q})$ .

REMARK 3.4. Assume that  $\text{III}(\mathbb{Q}, J_l)$  is finite. As  $C_l(\mathbb{Q}) \neq \emptyset$ , it follows from the work of Poonen and Stoll [18] that the Cassels–Tate pairing on  $\text{III}(\mathbb{Q}, J_l)$  is alternating, and so  $\#\text{III}(\mathbb{Q}, J_l)$  is a square. In this case, we find from the equality in (3.6) that  $\text{rank } J_l(\mathbb{Q})$  and  $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(\mathbb{Q}, J_l)$  have the same parity. Together with the fact that  $\text{rank } J_l(\mathbb{Q}) \geq 1$  we now see that we can read off  $\text{rank } J_l(\mathbb{Q})$  from Table 1 (still assuming the finiteness of  $\text{III}(\mathbb{Q}, J_l)$ , or actually just of the 2-part).

REMARK 3.5. Instead of using 2-descent on  $J_l/\mathbb{Q}$ , we can also apply [24], [26] to get an upper bound for  $\text{rank } J_l(\mathbb{Q})$  using  $(1 - \zeta_l)$ -descent on  $J_l/\mathbb{Q}(\zeta_l)$ . It turns out that for  $l = 7, 11$  this gives the same upper bound for  $\text{rank } J_l(\mathbb{Q})$  as given by Table 1 (namely 1 and 2 respectively). For  $l = 13, 17, 19$ , however, the upper bounds obtained from  $(1 - \zeta_l)$ -descent are strictly larger than the bounds given by Table 1.

For  $l = 7, 19$  both the Chabauty condition is satisfied and we have explicitly found a subgroup of finite index in the Mordell–Weil group  $J_l(\mathbb{Q})$ . We are thus in a position to use the method of Chabauty–Coleman to determine  $C_l(\mathbb{Q})$  for these  $l$ .

*Proof of Proposition 3.2.* Let  $l \in \{7, 19\}$  and let  $J_l$  denote, as before, the Jacobian of  $C_l$ . We already know that  $\text{rank } J_l(\mathbb{Q}) = 1$  and  $D := [(1, 5) - \infty] \in J_l(\mathbb{Q})$  generates a subgroup of finite index in  $J_l(\mathbb{Q})$ . We shall apply the method of Chabauty–Coleman, sketched in Section 2.1, with  $p = 3$ . A basis for  $\Omega(C_l/\mathbb{Q}_3)$  is given by  $X^i \frac{dX}{Y}$  with  $i = 0, 1, \dots, g_l - 1 = (l - 3)/2$ . For  $l = 7$  we find

$$\int_0^D \frac{dX}{Y} \equiv 3 \cdot 40, \quad \int_0^D X \frac{dX}{Y} \equiv 3^2 \cdot 25, \quad \int_0^D X^2 \frac{dX}{Y} \equiv 3^2 \cdot 13 \pmod{3^5}.$$

For  $l = 19$  we find the following congruences modulo  $3^5$ :

$$\left( \int_0^D X^k \frac{dX}{Y} \right)_{k=0}^8 \equiv (3 \cdot 43, 3 \cdot 76, 3 \cdot 16, 3 \cdot 22, 3 \cdot 65, 3 \cdot 74, 3^2 \cdot 17, 3^2 \cdot 23, 3^2 \cdot 22);$$

for hints on the evaluation of  $p$ -adic integrals see [27] (especially Section 1.9). Using these values, one can easily approximate an explicit basis



for  $\text{Ann}(J_l(\mathbb{Q}))$  in both cases. However, it is enough to notice that

$$\text{ord}_3\left(\int_0^D \frac{dX}{Y}\right) = 1, \quad \text{ord}_3\left(\int_0^D X^{g_l-1} \frac{dX}{Y}\right) = 2.$$

Thus we can find some  $\omega_l \in \text{Ann}(J_l(\mathbb{Q}))$  of the form

$$\omega_l = 3\alpha_l \frac{dX}{Y} + X^{g_l-1} \frac{dX}{Y}, \quad \alpha_l \in \mathbb{Z}_3, \quad \text{ord}_3(\alpha_l) = 0.$$

We reduce to obtain a differential on  $\tilde{C}_l/\mathbb{F}_3$ ,

$$\bar{\omega}_l = X^{g_l-1} \frac{dX}{Y}.$$

The differential  $\bar{\omega}_l$  does not vanish at any of the four points of  $C_l(\mathbb{F}_3)$ :

$$C_l(\mathbb{F}_3) = \{\infty, (\bar{1}, \bar{1}), (\bar{1}, \bar{2}), (\bar{2}, \bar{0})\}.$$

It follows that for each  $\tilde{P} \in C_l(\mathbb{F}_3)$  there is at most one  $P \in C_l(\mathbb{Q})$  that reduces to  $\tilde{P}$ . Now the rational points  $\infty$ ,  $(1, 5)$ , and  $(1, -5)$  respectively reduce to  $\infty$ ,  $(\bar{1}, \bar{2})$ ,  $(\bar{1}, \bar{1})$ .

To complete the proof it is sufficient to show that no  $\mathbb{Q}$ -rational point reduces to  $(\bar{2}, \bar{0})$ . One way of showing this is to use the Mordell–Weil sieve [4]. Here is a simpler method. Note that  $(\bar{2}, \bar{0})$  lifts to  $(\gamma, 0) \in C_l(\mathbb{Q}_3)$  where  $\gamma$  is the unique element in  $\mathbb{Q}_3$  satisfying  $\gamma^l = -1/4$ . Now the divisor  $D' = (\gamma, 0) - \infty$  has order 2 in  $J_l(\mathbb{Q}_p)$ , and hence belongs to the left-kernel of the pairing (2.1). If there is a  $\mathbb{Q}$ -rational point that reduces to  $(\bar{2}, \bar{0})$ , then that would force  $\bar{\omega}_l$  to vanish at  $(\bar{2}, \bar{0})$ . This completes the proof. Further details can be found in our MAGMA script `Chabauty551.m`. ■

**3.2. A modular approach to  $x^5 + y^5 = z^l$  when  $5 \mid z$ .** The purpose of this section is to give a proof of Proposition 3.3. Let  $(x, y, z)$  be a primitive integer solution to (1.2) with  $z \neq 0$  for some prime  $l \geq 7$  and assume  $5 \mid z$ . In this case Lemma 2.2 gives us  $\gcd(x + y, H_5) = 5$  and  $5^2 \nmid H_5$ . Hence (3.3) yields

$$5(x + y) = z_1^l, \quad H_5 = 5z_2^l$$

where  $z_1, z_2$  are coprime non-zero integers satisfying  $z = z_1 z_2$ .

Kraus [14, pp. 329–330] has constructed a Frey curve for the equation  $x^5 + y^5 = z^l$ . Following Kraus, we associate to our solution  $(x, y, z)$  to (1.2) the Frey elliptic curve

$$E'_{x,y} : Y^2 = X^3 + 5(x^2 + y^2)X^2 + 5H_5(x, y)X.$$

Since we are assuming that  $5 \mid z$ , we have  $5 \mid H_5(x, y)$ . So the quadratic twist over  $\mathbb{Q}(\sqrt{-5})$  given by the following model has integer coefficients:

$$E_{x,y} : Y^2 = X^3 - (x^2 + y^2)X^2 + \frac{H_5(x, y)}{5}X.$$

We record some of the invariants of  $E_{x,y}$ :

$$\begin{aligned} c_4 &= 2^4 \cdot 5^{-1} \cdot (2x^4 + 3x^3y + 7x^2y^2 + 3xy^3 + 2y^4) \in \mathbb{Z}, \\ c_6 &= 2^5 \cdot 5^{-1} \cdot (x^2 + y^2)(x^4 + 9x^3y + 11x^2y^2 + 9xy^3 + y^4) \in \mathbb{Z}, \\ \Delta &= 2^4 \cdot 5^{-3} \cdot (x + y)^4 H_5^2 = 2^4 \cdot 5^{-5} \cdot (z_1^2 z_2)^{2l} \in \mathbb{Z}, \\ j &= \frac{2^8 \cdot (2x^4 + 3x^3y + 7x^2y^2 + 3xy^3 + 2y^4)^3}{(x + y)^4 H_5^2}. \end{aligned}$$

LEMMA 3.6. *The conductor  $N$  and minimal discriminant  $\Delta_{\min}$  of  $E_{x,y}$  satisfy*

- $N = 2^\alpha 5 \operatorname{Rad}_{\{2,5\}}(z)$  where  $\alpha \in \{1, 3, 4\}$  and  $\operatorname{Rad}_{\{2,5\}}(z)$  is the product of the distinct primes not equal to 2 or 5 dividing  $z$ ;
- if  $2 \nmid z$ , then  $\Delta_{\min} = \Delta$ , and if  $2 \mid z$ , then  $\Delta_{\min} = \Delta/2^{12}$ .

*Proof.* Recall that  $x, y$  are coprime. The resultant of  $x^5 + y^5$  and  $2x^4 + 3x^3y + 7x^2y^2 + 3xy^3 + 2y^4$  is  $5^5$ . Thus any prime  $p \neq 2, 5$  dividing  $z$  cannot divide  $c_4$  and divides  $\Delta$ , and must therefore be a prime of multiplicative reduction. Using  $5 \mid z$ , we see that  $5 \mid \Delta$  and  $5 \nmid c_4$ . So 5 is also a prime of multiplicative reduction. Thus the conductor  $N$  is  $2^\alpha 5 \operatorname{Rad}_{\{2,5\}}(z)$  for some  $\alpha \in \mathbb{Z}_{\geq 0}$ . We also see that the model for  $E_{x,y}$  is minimal at any prime  $p \neq 2$ .

If  $2 \nmid z$ , then  $\operatorname{ord}_2(\Delta) = 4$ ,  $\operatorname{ord}_2(c_6) = 5$ , and  $\operatorname{ord}_2(c_4) \geq 5$ . So in this case the model for  $E_{x,y}$  is minimal at 2, and a straightforward application of Tate's algorithm [22, Section IV.9] gives  $\alpha \in \{3, 4\}$ . Finally, if  $2 \mid z$ , then  $\operatorname{ord}_2(\Delta) \geq 32$  and  $\operatorname{ord}_2(c_4) = 4$ . A straightforward application of Tate's algorithm shows that the model for  $E_{x,y}$  is not minimal at 2 and we get a new model  $E'$  that is integral at 2 with  $\operatorname{ord}_2(\Delta') = \operatorname{ord}_2(\Delta) - 12 \geq 20$  and  $\operatorname{ord}_2(c'_4) = \operatorname{ord}_2(c_4) - 4 = 0$ . So in this case  $E_{x,y}$  has multiplicative reduction at 2 and  $\Delta_{\min} = \Delta/2^{12}$ . ■

For a prime  $l$  we write  $\rho_l^{x,y}$  for the Galois representation on the  $l$ -torsion of  $E_{x,y}$ :

$$\rho_l^{x,y} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \operatorname{Aut}(E_{x,y}[l]).$$

LEMMA 3.7. *For primes  $l \geq 7$  the representation  $\rho_l^{x,y}$  is irreducible.*

*Proof.* Since  $E_{x,y}$  has a rational 2-isogeny, a reducible  $\rho_l^{x,y}$  (for an odd prime  $l$ ) would give rise to a non-cuspidal  $\mathbb{Q}$ -rational point on the modular curve  $X_0(2l)$ . By work of Mazur et al. (see e.g. [8, Section 2.1.2]) this is impossible for primes  $l \geq 11$ , and is only possible for  $l = 7$  if  $j \in \{-3^3 \cdot 5^3, 3^3 \cdot 5^3 \cdot 17^3\}$ . Using our explicit formula for the  $j$ -invariant of  $E_{x,y}$  we easily check that there are no  $[x : y] \in \mathbb{P}^1(\mathbb{Q})$  giving rise to one of these two values for  $j$ . ■

Now applying modularity and level lowering we deduce the following.

LEMMA 3.8. *For primes  $l \geq 7$  the Galois representation  $\rho_l^{x,y}$  arises from a newform  $f$  of level  $N = 2^\alpha 5$  where  $\alpha \in \{1, 3, 4\}$ .*

*Proof.* By [3] we see that  $\rho_l^{x,y}$  is modular of level  $N(E_{x,y})$ . Since by Lemma 3.7,  $\rho_l^{x,y}$  is also irreducible, we deduce by level lowering [19], [20] that  $\rho_l^{x,y}$  is modular of level  $N(E_{x,y})/M$  where  $M$  is the product of all primes  $p \parallel N(E_{x,y})$  with  $l \mid \text{ord}_p(\Delta_{\min}(E_{x,y}))$ . The possible values for  $N(E_{x,y})$  and  $\Delta_{\min}(E_{x,y})$  can be read off from Lemma 3.6. ■

We used MAGMA to compute the newforms at these levels; MAGMA uses Stein's [23] algorithms for this. We found respectively 0, 1, and 2 newforms at these levels, which are all rational. The (strong Weil) elliptic curves  $E_0$  corresponding to these newforms are  $E_{40a1}$ ,  $E_{80a1}$ , and  $E_{80b1}$ , where the subscript denotes the Cremona reference. We wrote a short MAGMA script `Modular551.m` which contains these, as well as the remaining computations of this section. Comparing traces of Frobenius as usual, gives the following.

LEMMA 3.9. *Suppose that  $\rho_l^{x,y} \simeq \rho_l^{E_0}$  for some prime  $l \geq 7$  and some  $E_0$  as above. Let  $p \neq 2, 5$  be a prime.*

- If  $p \nmid z$ , then  $a_p(E_0) \equiv a_p(E_{x,y}) \pmod{l}$ .
- If  $p \mid z$ , then  $a_p(E_0) \equiv \pm(1+p) \pmod{l}$ .

*Proof.* See e.g. [6, Propositions 15.2.2 and 15.2.3] or [8, Theorem 36]. ■

We will now finish our intended proof.

*Proof of Proposition 3.3.* By Lemma 3.8 and the determination of newforms of level  $2^\alpha 5$  where  $\alpha \in \{1, 3, 4\}$ , we know that  $\rho_l^{x,y} \simeq \rho_l^{E_0}$  for some prime  $l \geq 7$  and  $E_0$  one of  $E_{40a1}$ ,  $E_{80a1}$ ,  $E_{80b1}$ . We will eliminate these three possibilities for  $E_0$ , which then proves the proposition. Let  $p \neq 2, 5$  denote a prime and define the sets

$$A_p := \{p+1 - \#E_{a,b}(\mathbb{F}_p) : a, b \in \mathbb{F}_p, a^5 + b^5 \neq 0\}, \quad T_p := A_p \cup \{\pm(1+p)\}.$$

Obviously, if  $p \nmid z$ , then  $a_p(E_{x,y}) \in A_p$ . Hence by Lemma 3.9 we have

$$(3.7) \quad a_p(E_0) \equiv t \pmod{l} \quad \text{for some } t \in T_p.$$

We compute

$$T_3 = \{\pm 2, \pm 4\}.$$

However,  $E_{40a1}$  and  $E_{80a1}$  have full 2-torsion, and so  $a_3(E_{40a1}) = a_3(E_{80a1}) = 0$ . Thus for  $l \geq 7$  prime and  $E_0$  one of  $E_{40a1}$  or  $E_{80a1}$ , we see that (3.7) with  $p = 3$  does not hold, and consequently  $\rho_l^{x,y} \not\simeq \rho_l^{E_0}$ . To deal with the remaining case  $E_0 = E_{80b1}$ , we compute

$$T_{43} = \{-44, -10, -8, -6, -2, 0, 2, 4, 6, 8, 12, 44\}, \quad a_{43}(E_{80b1}) = 10.$$

Now (3.7) does not hold for any prime  $l \geq 7$ , *except* for  $l = 17$ . So from now on let  $l = 17$ . We deal with this case using the method of Kraus. For a prime  $p \equiv 1 \pmod{l}$ , let  $(\mathbb{F}_p^*)^l$  denote the non-zero  $l$ th powers in  $\mathbb{F}_p$  and define the sets

$$\begin{aligned} A'_{p,l} &:= \{p+1 - \#E_{a,b}(\mathbb{F}_p) : a, b \in \mathbb{F}_p, 5(a+b) \in (\mathbb{F}_p^*)^l, H_5(a,b)/5 \in (\mathbb{F}_p^*)^l\}, \\ T'_{p,l} &:= A'_{p,l} \cup \{\pm 2\}. \end{aligned}$$

Now take  $p = 6 \cdot 17 + 1 = 103$ . Since we are assuming  $\rho_{17}^{x,y} \simeq \rho_{17}^{E_0}$  (with  $E_0 = E_{80b1}$ ), Lemma 3.9 tells us that

$$(3.8) \quad a_{103}(E_{80b1}) \equiv t \pmod{17} \quad \text{for some } t \in T'_{103,17}.$$

We compute

$$T'_{103,17} = \{-6, \pm 2\}, \quad a_{103}(E_{80b1}) = -14,$$

and conclude that (3.8) does not hold, which completes the proof. ■

**3.3. Necessity of the modular approach.** Proving the non-existence of non-trivial primitive integer solutions to (1.2) with  $5|z$  for some odd prime  $l$  can be reduced to finding  $\mathbb{Q}$ -rational points on the hyperelliptic curve

$$D_l : Y^2 = 4X^l + 5^{2l-5}.$$

Note that this curve has genus  $(l-1)/2$  and that

$$D_l(\mathbb{Q}) \supset \{\infty\}.$$

LEMMA 3.10. *Let  $l$  be an odd prime. If*

$$(3.9) \quad D_l(\mathbb{Q}) = \{\infty\},$$

*then there are no non-trivial primitive integer solutions to (1.2) with  $5|z$ .*

*Proof.* In this case Lemma 2.2 gives us  $\gcd(x+y, H_5) = 5$  and  $5^2 \nmid H_5$ . Hence (3.3) yields

$$5(x+y) = z_1^l, \quad H_5 = 5z_2^l$$

where  $z_1, z_2$  are coprime non-zero integers satisfying  $z = z_1 z_2$ . Using identity (3.4) we see that

$$5(x^2 + y^2)^2 = 20z_2^l + 5^{-4}z_1^{4l}.$$

Multiplying both sides by  $5^{2l-1}/z_1^{4l}$  gives

$$\left( \frac{5^l(x^2 + y^2)}{z_1^{2l}} \right)^2 = 4 \left( \frac{5^2 z_2}{z_1^4} \right)^l + 5^{2l-5}.$$

Thus

$$P = \left( \frac{5^2 z_2}{z_1^4}, \frac{5^l(x^2 + y^2)}{z_1^{2l}} \right) \in D_l(\mathbb{Q}).$$

Since  $z_1 \neq 0$ , we have  $P \neq \infty$ . This proves the lemma. ■

Upper bounds for  $\text{rank Jac}(D_l)(\mathbb{Q})$  are given by the 2-Selmer ranks of  $\text{Jac}(D_l)/\mathbb{Q}$ ; see Table 2. For  $l = 7$  and  $l = 13$  (and, assuming GRH, also for  $l = 17$ ) we conclude that  $\text{rank Jac}(D_l)(\mathbb{Q}) = 0$ , so it is easy to determine  $D_l(\mathbb{Q})$  for these values of  $l$ . Since our focus is on  $l = 7, 19$ , we give the details for  $l = 7$ .

REMARK 3.11. Instead of using 2-descent on  $\text{Jac}(D_l)/\mathbb{Q}$ , we can also apply [24], [26] to get an upper bound for  $\text{rank Jac}(D_l)(\mathbb{Q})$  using  $(1 - \zeta_l)$ -descent on  $\text{Jac}(D_l)/\mathbb{Q}(\zeta_l)$ . It turns out that for  $l = 11$  this gives the same upper bound for  $\text{rank Jac}(D_l)(\mathbb{Q})$  as given by Table 2 (namely 3). For  $l = 7, 13, 17, 19$ , however, the upper bounds obtained from  $(1 - \zeta_l)$ -descent will be strictly larger than the bounds given by Table 2 (but one does not need to assume GRH).

**Table 2.** Rank bounds for the Jacobian of  $D_l$

$l$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(\mathbb{Q}, \text{Jac}(D_l))$ <sup>(a)</sup>	Time
7	0	1.4 s
11	3	2093 s
13	0	264613 s $\approx$ 3.1 days
17	0*	240 s
19	1*	723 s

<sup>(a)</sup> The \* indicates that the result is conditional on GRH.

LEMMA 3.12. *The only  $\mathbb{Q}$ -rational point on  $D_7$  is the single point at infinity.*

*Proof.* Let  $J$  denote the Jacobian of  $D_7$ . We shall show that  $J(\mathbb{Q}) = \{0\}$ . Since the Abel–Jacobi map

$$D_7 \rightarrow J, \quad P \mapsto [P - \infty],$$

is injective, it will follow that  $D_7(\mathbb{Q}) = \{\infty\}$ .

First we determine the torsion subgroup  $J(\mathbb{Q})_{\text{tors}}$  of  $J(\mathbb{Q})$ . The curve  $D_7$ , and hence its Jacobian  $J$ , has good reduction away from 2, 5, 7. For any (necessarily odd) prime  $p$  of good reduction, the natural map

$$J(\mathbb{Q})_{\text{tors}} \rightarrow J(\mathbb{F}_p)$$

is injective. Using MAGMA we find that

$$\#J(\mathbb{F}_3) = 28, \quad \#J(\mathbb{F}_{43}) = 39929.$$

Since  $\text{gcd}(28, 39929) = 1$ , we deduce that  $J(\mathbb{Q})_{\text{tors}} = \{0\}$ .

We have already seen that  $\text{rank } J(\mathbb{Q}) = 0$ . It follows that  $J(\mathbb{Q}) = \{0\}$ , which completes the proof. ■

Let  $r := \text{rank Jac}(D_{19})(\mathbb{Q})$ . We see from Table 2 that  $r \leq 1$  under the assumption of GRH. Assuming the finiteness of  $\text{III}(\mathbb{Q}, \text{Jac}(D_{19}))$  in addition to GRH leads to  $r = 1$ . So in order to use the method of Chabauty–Coleman to determine  $D_{19}(\mathbb{Q})$ , we must first of all prove that  $r = 1$  (if true...) and next find a  $\mathbb{Q}$ -rational point of infinite order on  $\text{Jac}(D_{19})$ . Both tasks seem quite challenging at the moment.

We conclude that the modular method is not necessary to prove Theorem 1 for the case  $l = 7$ , but that for  $l = 19$  we really do need it at this point.

**4. Proof of Theorem 2.** In this section we shall be concerned with the primitive integer solutions to (1.3) for primes  $l \neq 2, 3, 7$ . Although ultimately we will only be able to (unconditionally) determine all the solutions if  $l = 5$ , we will take a more general approach. The reason for doing this is threefold. First of all, it is simply not much more work to consider more values of  $l$ . Second, while we do not fully determine (unconditionally) all primitive integer solutions to (1.3) for any prime  $l \geq 11$ , we do obtain many other partial results for  $l \geq 11$ , which may be interesting in their own right. Finally, in Section 5 we solve (1.3) for  $l = 11$  assuming GRH, for which we lay the foundations here.

**4.1. Initial factorizations for  $x^7 + y^7 = z^l$ .** Let  $(x, y, z)$  be a primitive integer solution to (1.3) for some prime  $l \neq 2, 3, 7$  and suppose that  $z \neq 0$ . Recall that

$$H_7(x, y) = \frac{x^7 + y^7}{x + y} = x^6 - x^5y + x^4y^2 - x^3y^3 + x^2y^4 - xy^5 + y^6.$$

By Lemma 2.2,  $\gcd(x + y, H_7(x, y)) = 1$  or  $7$  and  $7^2 \nmid H_7(x, y)$ . Thus we can again subdivide into two cases:

- If  $7 \nmid z$ , then

$$(4.1) \quad x + y = z_1^l, \quad H_7(x, y) = z_2^l, \quad z = z_1 z_2,$$

where  $z_1, z_2$  are non-zero, coprime integers.

- If  $7 \mid z$ , then

$$(4.2) \quad 7(x + y) = z_1^l, \quad H_7(x, y) = 7z_2^l, \quad z = z_1 z_2,$$

where  $z_1, z_2$  are non-zero, coprime integers.

These factorizations do not seem to be sufficient to enable us to solve the problem. Henceforth,  $\zeta$  will denote a primitive 7th root of unity,  $L = \mathbb{Q}(\zeta)$  and  $\mathcal{O} = \mathbb{Z}[\zeta]$  the ring of integers of  $L$ . The class number of  $\mathcal{O}$  is 1 and the unit rank is 2. The unit group is in fact

$$\{\pm \zeta^i (1 + \zeta)^r (1 + \zeta^2)^s : 0 \leq i \leq 6, r, s \in \mathbb{Z}\}.$$

Moreover, 7 ramifies as  $7\mathcal{O} = (1 - \zeta)^6\mathcal{O}$ . Now  $H_7(x, y) = \text{Norm}(x + \zeta y)$ . From (4.1) and (4.2) we have

- If  $7 \nmid z$ , then

$$(4.3) \quad x + \zeta y = (1 + \zeta)^r(1 + \zeta^2)^s\beta^l, \quad 0 \leq r, s \leq l - 1,$$

for some  $\beta \in \mathbb{Z}[\zeta]$ .

- If  $7 \mid z$ , then

$$(4.4) \quad x + \zeta y = (1 - \zeta)(1 + \zeta)^r(1 + \zeta^2)^s\beta^l, \quad 0 \leq r, s \leq l - 1,$$

for some  $\beta \in \mathbb{Z}[\zeta]$ .

Thus we have  $2l^2 \geq 50$  cases to consider. In the next section we will use the modular approach to reduce the number of cases to just two for many values of  $l$ , e.g.  $l = 5, 11$ .

**4.2. A modular approach to  $x^7 + y^7 = z^l$ .** Consider the subset of primes

$$L_7 := \{\text{primes } l : l \neq 2, 3, 7 \text{ and } l < 100\}.$$

The purpose of this section is to prove the following proposition.

**PROPOSITION 4.1.** *Let  $(x, y, z)$  be a primitive integer solution to (1.3) with  $z \neq 0$  and  $l \in L_7$ . If  $7 \nmid z$ , then (4.3) holds with  $r = s = 0$ . If  $7 \mid z$ , then (4.4) holds with  $r = s = 0$ .*

Let  $(x, y, z)$  be a primitive integer solution to (1.3) with  $z \neq 0$  for some prime  $l \geq 5$ ,  $l \neq 7$ . Kraus [14, pp. 329–330] constructed a Frey curve for the equation  $x^7 + y^7 = z^l$ . Following Kraus, we associate to our solution  $(x, y, z)$  to (1.3) the Frey elliptic curve

$$E_{x,y} : Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

where

$$\begin{aligned} a_2 &= -(x - y)^2, & a_4 &= -2x^4 + x^3y - 5x^2y^2 + xy^3 - 2y^4, \\ a_6 &= x^6 - 6x^5y + 8x^4y^2 - 13x^3y^3 + 8x^2y^4 - 6xy^5 + y^6. \end{aligned}$$

We record some of the invariants of  $E_{x,y}$ :

$$(4.5) \quad c_4 = 2^4 \cdot 7(x^4 - x^3y + 3x^2y^2 - xy^3 + y^4),$$

$$(4.6) \quad c_6 = -2^5 \cdot 7(x^6 - 15x^5y + 15x^4y^2 - 29x^3y^3 + 15x^2y^4 - 15xy^5 + y^6),$$

$$(4.7) \quad \Delta = 2^4 \cdot 7^2 H_7(x, y)^2, \quad j = \frac{2^8 \cdot 7(x^4 - x^3y + 3x^2y^2 - xy^3 + y^4)^3}{H_7(x, y)^2}.$$

**LEMMA 4.2.** *The conductor  $N$  and minimal discriminant  $\Delta_{\min}$  of  $E_{x,y}$  satisfy*

- $N = 2^\alpha 7^2 \text{Rad}(z_2)$  where  $\alpha = 2$  or  $3$  and  $\text{Rad}(z_2)$  is the product of the distinct primes dividing  $z_2$  (and  $2, 7 \nmid z_2$ );
- $\Delta_{\min} = \Delta$ .

*Proof.* Recall that  $x, y$  are coprime. The resultant of  $H_7(x, y)$  and  $x^4 - x^3y + 3x^2y^2 - xy^3 + y^4$  is  $7^2$ . Thus any prime  $p \neq 2, 7$  dividing  $H_7(x, y)$  cannot divide  $c_4$  and divides  $\Delta$ , and must therefore be a prime of multiplicative reduction. We know that  $H_7(x, y) = 7z_2^l$  or  $H_7(x, y) = z_2^l$ . Moreover,  $7^2 \nmid H_7(x, y)$ , so  $7 \nmid z_2$ . Thus the conductor  $N$  is  $\text{Rad}(z_2)$  up to powers of 2 and 7. We also see that the model for  $E_{x,y}$  is minimal at any prime  $p \neq 2, 7$ .

Now  $\text{ord}_7(\Delta) = 4$  or  $2$ . Hence the model for  $E_{x,y}$  is minimal at 7. Since  $7 \mid c_4$ , we see that  $E_{x,y}$  has additive reduction at 7, and so  $\text{ord}_7(N) = 2$ .

Finally, as  $x, y$  are coprime we quickly get  $\text{ord}_2(c_4) = 4$ ,  $\text{ord}_2(c_6) = 5$  as well as  $\text{ord}_2(\Delta) = 4$ . Thus the model for  $E_{x,y}$  is also minimal at 2 and we conclude that  $\Delta_{\min} = \Delta$ . Note that  $E_{x,y} = E_{y,x}$ . Without loss of generality we may suppose that either  $x$  is even or  $z$  is even. Applying Tate's algorithm [22, Section IV.9] shows the following:

- (a) if  $2 \mid z$ , then  $\text{ord}_2(N) = 3$ ;
- (b) if  $2 \parallel x$ , then  $\text{ord}_2(N) = 3$ ;
- (c) if  $4 \mid x$ , then  $\text{ord}_2(N) = 2$ .

This completes the proof. ■

We shall write  $\rho_l^{x,y}$  for the Galois representation on the  $l$ -torsion of  $E_{x,y}$ :

$$\rho_l^{x,y} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E_{x,y}[l]).$$

LEMMA 4.3. *For  $l = 5$  or primes  $l \geq 11$  the representation  $\rho_l^{x,y}$  is irreducible.*

*Proof.* If  $l = 11$  or  $l \geq 17$ , then, by work of Mazur et al. on the  $\mathbb{Q}$ -rational points of  $X_0(l)$ , the irreducibility follows by checking that the  $j$ -invariant of  $E_{x,y}$  does not belong to an explicit list of 11 values; see e.g. [8, Theorem 22].

Now let  $l \in \{5, 13\}$  and suppose that  $\rho_l^{x,y}$  is reducible. Then the  $j$ -invariant of  $E_{x,y}$  must be in the image of  $X_0(l)(\mathbb{Q})$  under the  $j$  map  $X_0(l) \rightarrow X(1)$ . In [8, Section 3.2] this  $j$  map is given explicitly as

$$(4.8) \quad j = \begin{cases} (t^2 + 10t + 5)^3/t & \text{if } l = 5, \\ (t^4 + 7t^3 + 20t^2 + 19t + 1)^3(t^2 + 5t + 13)/t & \text{if } l = 13. \end{cases}$$

In other words, this equation must have a  $\mathbb{Q}$ -rational solution  $t$  where  $j$  is the  $j$ -invariant of  $E_{x,y}$ . It is clear from (4.7) that  $\text{ord}_2(j) = 8$ . It is easy to see that this is impossible from (4.8). This completes the proof. Alternatively, the irreducibility for  $l \in \{5, 13\}$  follows immediately from [8, Theorem 60 and Table 3.1] with  $F(u, v) = u^3 - u^2v - 2uv^2 + v^3$  and the remark that  $F(x^2 + y^2, xy) = H_7(x, y)$ . ■

Using Lemmata 4.2 and 4.3 we can apply modularity [3] and level lowering [19], [20] as usual, to deduce the following.



LEMMA 4.4. *For a prime  $l \neq 2, 3, 7$ , the Galois representation  $\rho_l^{x,y}$  arises from a newform  $f$  of level  $N = 2^\alpha 7^2$  where  $\alpha = 2$  or  $3$ .*

We again used MAGMA to compute the newforms at these levels. We found respectively 3 and 8 newforms (up to Galois conjugacy) there. Of these, 2 and 6 respectively are rational newforms and therefore correspond to elliptic curves. We wrote a short MAGMA script `Modular771.m` which contains them, as well as the remaining computations of this section. Our first step is to eliminate as many of the newforms above as possible.

LEMMA 4.5. *Suppose  $\rho_l^{x,y}$  arises from a newform*

$$(4.9) \quad f = q + \sum_{i \geq 2} a_i(f)q^i.$$

*Let  $K = \mathbb{Q}(a_2(f), a_3(f), \dots)$  be the number field generated by the coefficients of  $f$ . Let  $p \neq 2, 7$  be prime. If  $K \neq \mathbb{Q}$ , we also impose  $p \neq l$ .*

- *If  $p \nmid z_2$ , then  $l \mid \text{Norm}_{K/\mathbb{Q}}(a_p(E_{x,y}) - a_p(f))$ .*
- *If  $p \mid z_2$ , then  $l \mid \text{Norm}_{K/\mathbb{Q}}((p+1)^2 - a_p(f)^2)$ .*

*Proof.* This follows from comparing traces of Frobenius; see e.g. [6, Propositions 15.2.2 and 15.2.3] or [8, Theorem 36]. ■

Specializing  $E_{x,y}$  at a trivial primitive integer solution with  $xy = 0$  (i.e.  $(x, y) = (\pm 1, 0)$  or  $(0, \pm 1)$ ) yields  $E_{196a1}$ , and specializing at a trivial primitive integer solution with  $z = 0$  (i.e.  $(x, y) = (\pm 1, \mp 1)$ ) yields  $E_{392c1}$ . Using the basic congruences from the lemma above, we can quickly eliminate all the (Galois conjugacy classes of) newforms at the levels 196 and 392 for all  $l$  simultaneously, except of course the two newforms corresponding to the two elliptic curves we just obtained by specialization of  $E_{x,y}$ .

LEMMA 4.6. *For a prime  $l \neq 2, 3, 7$ , the Galois representation  $\rho_l^{x,y}$  arises from  $E_{196a1}$  or  $E_{392c1}$ .*

*Proof.* By Lemma 4.4 we see that  $\rho_l^{x,y}$  arises from a newform  $f$  of level  $2^\alpha 7^2$  where  $\alpha = 2$  or  $3$ . Let  $p \neq 2, 7$  denote a prime and define the sets

$$A_p := \{p+1 - \#E_{a,b}(\mathbb{F}_p) : a, b \in \mathbb{F}_p, H_7(a, b) \neq 0\},$$

$$T_p := \begin{cases} A_p & \text{if } p \not\equiv 1 \pmod{7}, \\ A_p \cup \{\pm(1+p)\} & \text{if } p \equiv 1 \pmod{7}. \end{cases}$$

Obviously, if  $p \nmid z_2$ , then  $a_p(E_{x,y}) \in A_p$ . Furthermore,  $p \equiv 1 \pmod{7}$  if and only if  $p$  splits completely in  $\mathbb{Z}[\zeta]$  if and only if  $H_7(a, b) = 0$  for some  $a, b \in \mathbb{F}_p$  not both zero (for this last step we use  $p \neq 7$ ). So we deduce from Lemma 4.5 that for any prime  $p \neq 2, 7$ ,

$$(4.10) \quad l \mid \text{Norm}_{K/\mathbb{Q}}(a_p(f) - t) \quad \text{for some } t \in T_p$$

or, in case  $K \neq \mathbb{Q}$ , that  $l = p$ .

If  $f$  is not rational, then we compute that  $a_3(f) \in \{\pm\sqrt{2}, \pm\sqrt{8}\}$  and  $T_3 = \{-1, 3\}$ . In this case (4.10) with  $p = 3$  reduces to  $l = 7$ , hence  $l = 7$  or  $l = p = 3$ . Since  $l = 3, 7$  are values outside our consideration, we conclude that we have eliminated the possibility that  $\rho_l^{x,y}$  arises from a non-rational newform. Similarly, for any rational newform  $f$  (of level  $2^\alpha 7^2$  where  $\alpha \in \{2, 3\}$ ) not corresponding to either of  $E_{196a1}$ ,  $E_{392c1}$ , we can find a single prime  $p \leq 23$ ,  $p \neq 2, 7$ , such that (4.10) does not hold for any prime  $l \neq 2, 3, 7$ . To be specific, for the rational newforms corresponding to an elliptic curve whose isogeny class has Cremona reference one of  $196b, 392a, 392b, 392f$  we can take  $p = 3$ , and for the isogeny classes given by  $392e, 392d$  we can take  $p = 11, 13$  respectively. ■

So far we have not distinguished between the cases  $7 \nmid z$  and  $7 \mid z$ . To refine the lemma above with respect to these two cases we can use the following.

LEMMA 4.7. *Let  $E_1, E_2$  be elliptic curves over  $\mathbb{Q}$  with potentially good reduction at a prime  $p \geq 5$ . If  $\gcd(12, \text{ord}_p(\Delta(E_1))) \neq \gcd(12, \text{ord}_p(\Delta(E_2)))$ , then for all primes  $l \neq 2, p$  we have  $\rho_l^{E_1} \not\cong \rho_l^{E_2}$ .*

*Proof.* This follows by comparing images of inertia; see e.g. [13]. ■

We can now strengthen Lemma 4.6 as follows.

LEMMA 4.8. *Let  $l \neq 2, 3, 7$  be prime. If  $7 \nmid z$ , then  $\rho_l^{x,y}$  arises from  $E_{196a1}$ . If  $7 \mid z$ , then  $\rho_l^{x,y}$  arises from  $E_{392c1}$ .*

*Proof.* Considering  $F := x^4 - x^3y + 3x^2y^2 - xy^3 + y^4$  modulo 7, we deduce that  $7 \mid F$  if and only if  $7 \mid H_7$ . Since  $7^2 \nmid H_7$ , we find from the invariants of  $E_{x,y}$  that  $\text{ord}_7(j) \geq 1$ , so  $E_{x,y}$  has potentially good reduction at 7. Furthermore, if  $7 \nmid z$ , then  $\text{ord}_7(\Delta) = 2$ , and if  $7 \mid z$ , then  $\text{ord}_7(\Delta) = 4$ . The curves  $E_{196a1}$  and  $E_{392c1}$  also have potentially good reduction at 7, and finally  $\text{ord}_7(\Delta(E_{196a1})) = 2$  and  $\text{ord}_7(\Delta(E_{392c1})) = 4$ . The assertion follows from Lemma 4.7. ■

REMARK 4.9. To prove Lemma 4.8 we used image of inertia arguments. It turns out that one can also eliminate  $E_{196a1}$  when  $7 \mid z$  for, say,  $l < 100$  with a simple application of Kraus' method. The curve  $E_{392c1}$  (when  $7 \nmid z$ ) is not susceptible to this method.

We now turn our attention to a result involving the exponents  $(r, s)$  in (4.3) and (4.4), after which we will complete the proof of Proposition 4.1.

LEMMA 4.10. *Let  $E_0/\mathbb{Q}$  be an elliptic curve, let  $p \neq 2, 7$  be prime, let  $l \neq 2, 3, 7$  be prime, and let  $g \in \{1, 7\}$ . Denote by  $\mathcal{A}_g(E_0, p)$  the set of  $(a, b) \in \mathbb{F}_p^2 - \{0, 0\}$  such that  $(a + b)g$  and  $H_7(a, b)/g$  are both  $l$ th powers*

in  $\mathbb{F}_p$ , and

- either  $H_7(a, b) \neq 0$  and  $a_p(E_0) \equiv a_p(E_{a,b}) \pmod{l}$ ,
- or  $H_7(a, b) = 0$  and  $a_p(E_0)^2 \equiv (p+1)^2 \pmod{l}$ .

Let  $\mathfrak{P}_1, \dots, \mathfrak{P}_m$  be the prime ideals of  $\mathbb{Z}[\zeta]$  dividing  $p$ . Write  $\kappa_i$  for the residue class field  $\mathbb{Z}[\zeta]/\mathfrak{P}_i$  and  $\pi_i$  for the corresponding natural map

$$\pi_i : \mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta] \rightarrow \kappa_i.$$

Denote by  $\mathcal{B}_g(E_0, p)$  the set of pairs  $(\mu, \eta)$  with  $0 \leq \mu, \eta < l$  such that there exists  $(a, b) \in \mathcal{A}_g(E_0, p)$  with

$$\pi_i \left( \frac{a + b\zeta}{(1 - \zeta)^{\text{ord}_7(g)}(1 + \zeta)^\mu(1 + \zeta^2)^\eta} \right)$$

an  $l$ th power in  $\kappa_i$  for  $i = 1, \dots, m$ .

- (a) If  $E_{x,y}$  arises from  $E_0$  and  $7 \nmid z$ , then (4.3) holds for some  $(r, s)$  in  $\mathcal{B}_1(E_0, p)$ .
- (b) If  $E_{x,y}$  arises from  $E_0$  and  $7 \mid z$ , then (4.4) holds for some  $(r, s)$  in  $\mathcal{B}_7(E_0, p)$ .

*Proof.* Let  $g := \gcd(x + y, H_7(x, y))$ . By Lemma 4.5 and (4.1) and (4.2) we see that if  $\rho_l^{x,y}$  arises from  $E_0$ , then  $(x, y) \equiv (a, b) \pmod{l}$  for some  $(a, b) \in \mathcal{A}_g(E_0, p)$ . The statement now follows directly by taking into account that the factorization of  $x^7 + y^7$  in  $\mathbb{Z}[\zeta]$  yields (4.3) and (4.4). ■

*Proof of Proposition 4.1.* Let  $(x, y, z)$  be a primitive integer solution to (1.3) with  $l \in L_7$ . We know that for some  $0 \leq r, s < l$  we have (4.3) if  $7 \nmid z$  and (4.4) if  $7 \mid z$ . Moreover, from Lemma 4.8 we know that  $\rho_l^{x,y}$  arises from  $E_{196a1}$  if  $7 \nmid z$  and from  $E_{392c1}$  if  $7 \mid z$ . By Lemma 4.10, for any prime  $p \neq 2, 7$ , if  $7 \nmid z$ , then

$$(r, s) \in \mathcal{B}_1(E_{196a1}, p),$$

and if  $7 \mid z$ , then

$$(r, s) \in \mathcal{B}_7(E_{392c1}, p).$$

We wrote a short MAGMA script to compute  $\mathcal{B}_g(E_0, p)$ . We found that for every prime  $l \in L_7$  there exist primes  $p_1, p_2$  such that

$$\mathcal{B}_1(E_{196a1}, p_1) = (0, 0) \quad \text{and} \quad \mathcal{B}_7(E_{392c1}, p_2) = (0, 0).$$

This proves the proposition (see the MAGMA script `Modular771.m` for more details). ■

**4.3. The hyperelliptic curves.** Assume  $l \in L_7$  and let  $(x, y, z)$  be a primitive integer solution to  $x^7 + y^7 = z^l$  with  $z \neq 0$ . Then according to Proposition 4.1 we have

$$(4.11) \quad x + \zeta y = \epsilon \beta^l, \quad d(x + y) = z_1^l$$

where  $\beta \in \mathbb{Z}[\zeta]$  and

$$(d, \epsilon) = \begin{cases} (1, 1) & \text{if } 7 \nmid z, \\ (7, 1 - \zeta) & \text{if } 7 \mid z. \end{cases}$$

Let  $\theta = \zeta + \zeta^{-1}$  and  $K = \mathbb{Q}(\theta)$ ; this is the totally real cyclic cubic subfield of  $L$ . The Galois conjugates of  $\theta$  are  $\theta_1, \theta_2, \theta_3$ , which in terms of  $\zeta$  are given by

$$\theta_1 = \zeta + \zeta^{-1}, \quad \theta_2 = \zeta^2 + \zeta^{-2}, \quad \theta_3 = \zeta^3 + \zeta^{-3}.$$

Note that

$$\theta_1 = \theta, \quad \theta_2 = \theta^2 - 2, \quad \theta_3 = -\theta^2 - \theta + 1.$$

Let

$$\mu = \text{Norm}_{L/K}(\epsilon), \quad \gamma = \text{Norm}_{L/K}(\beta).$$

Taking norms in (4.11) down to  $K$  we obtain

$$(4.12) \quad x^2 + \theta xy + y^2 = \mu \gamma^l, \quad d(x + y) = z_1^l$$

where  $\gamma \in \mathcal{O}_K$  and

$$(d, \mu) = \begin{cases} (1, 1) & \text{if } 7 \nmid z, \\ (7, 2 - \theta) & \text{if } 7 \mid z. \end{cases}$$

Let  $\mu_1 = \mu, \mu_2, \mu_3$  denote the conjugates of  $\mu$  that correspond respectively to  $\theta \mapsto \theta_j$  for  $j = 1, 2, 3$ . Likewise let  $\gamma_1, \gamma_2, \gamma_3$  be the corresponding conjugates of  $\gamma$ . Then

$$x^2 + \theta_1 xy + y^2 = \mu_1 \gamma_1^l, \quad x^2 + \theta_2 xy + y^2 = \mu_2 \gamma_2^l, \quad x^2 + \theta_3 xy + y^2 = \mu_3 \gamma_3^l.$$

Furthermore, recall that

$$(x + y)^2 = d^{-2} z_1^{2l} \quad \text{where} \quad d = \begin{cases} 1 & \text{if } 7 \nmid z, \\ 7 & \text{if } 7 \mid z. \end{cases}$$

The left-hand sides of the previous four equations are symmetric binary quadratic forms over  $K$ . Since such forms obviously form a 2-dimensional vector space over  $K$ , there exist linear relations between the four forms. We calculate

$$\begin{aligned} (x + y)^2 + \theta_2(x^2 + \theta_1 xy + y^2) + \theta_3(x^2 + \theta_2 xy + y^2) + \theta_1(x^2 + \theta_3 xy + y^2) &= 0, \\ (x + y)^2 + \theta_3(x^2 + \theta_1 xy + y^2) + \theta_1(x^2 + \theta_2 xy + y^2) + \theta_2(x^2 + \theta_3 xy + y^2) &= 0. \end{aligned}$$

This yields nice equations for a curve in projective 3-space in the coordinates  $z_1^2, \gamma_1, \gamma_2, \gamma_3$ :

$$\begin{aligned} d^{-2} z_1^{2l} + \theta_2 \mu_1 \gamma_1^l + \theta_3 \mu_2 \gamma_2^l + \theta_1 \mu_3 \gamma_3^l &= 0, \\ d^{-2} z_1^{2l} + \theta_3 \mu_1 \gamma_1^l + \theta_1 \mu_2 \gamma_2^l + \theta_2 \mu_3 \gamma_3^l &= 0. \end{aligned}$$

We can eliminate one of the  $\gamma_i$ , say  $\gamma_3$ , to get

$$(4.13) \quad (\theta_2 - \theta_1) d^{-2} z_1^{2l} + (\theta_2^2 - \theta_1 \theta_3) \mu_1 \gamma_1^l + (\theta_2 \theta_3 - \theta_1^2) \mu_2 \gamma_2^l = 0.$$

And a projective plane curve in the coordinates  $\gamma_1, \gamma_2, \gamma_3$  is quickly obtained as

$$(4.14) \quad (\theta_2 - \theta_3)\mu_1\gamma_1^l + (\theta_3 - \theta_1)\mu_2\gamma_2^l + (\theta_1 - \theta_2)\mu_3\gamma_3^l = 0.$$

REMARK 4.11. Let  $\alpha_1, \alpha_2, \alpha_3$  be non-zero elements in a field  $F$  of characteristic 0 and consider the non-singular plane projective curve over  $F$  determined by the equation

$$(4.15) \quad \alpha_1u^l + \alpha_2v^l + \alpha_3w^l = 0.$$

Using the identity

$$(\alpha_1u^l - \alpha_2v^l)^2 = (\alpha_1u^l + \alpha_2v^l)^2 - 4\alpha_1\alpha_2(uv)^l,$$

we deduce from (4.15) that

$$(\alpha_1u^l - \alpha_2v^l)^2 = -4\alpha_1\alpha_2(uv)^l + \alpha_3^2w^{2l}.$$

By dividing both sides by  $\alpha_3^2w^{2l}$ , we see that

$$\left( \frac{uv}{w^2}, \frac{\alpha_1u^l - \alpha_2v^l}{\alpha_3w^l} \right) \in C(F)$$

where  $C$  is the genus  $(l-1)/2$  hyperelliptic curve determined by

$$C : Y^2 = -4\eta X^l + 1, \quad \eta = \alpha_1\alpha_2/\alpha_3^2.$$

Obviously, by permuting the indices, we find that  $F$ -rational points on (4.15) also give rise to  $F$ -rational points on the hyperelliptic curves given by the equation above with  $\eta = \alpha_2\alpha_3/\alpha_1^2$  and  $\eta = \alpha_3\alpha_1/\alpha_2^2$  respectively.

Define

$$\begin{aligned} \alpha_1 &:= (\theta_2 - \theta_1)d^{-2}, & \alpha_2 &:= (\theta_2^2 - \theta_1\theta_3)\mu_1, & \alpha_3 &:= (\theta_2\theta_3 - \theta_1^2)\mu_2; \\ \alpha'_1 &:= (\theta_2 - \theta_3)\mu_1, & \alpha'_2 &:= (\theta_3 - \theta_1)\mu_2, & \alpha'_3 &:= (\theta_1 - \theta_2)\mu_3; \\ \eta_1 &:= \alpha_2\alpha_3/\alpha_1^2, & \eta_2 &:= \alpha_3\alpha_1/\alpha_2^2, & \eta_3 &:= \alpha_1\alpha_2/\alpha_3^2, & \eta_4 &:= \alpha'_1\alpha'_2/\alpha_3'^2. \end{aligned}$$

Then we see that Remark 4.11 above leads to  $K$ -rational points on the curves

$$Y^2 = -4\eta_i X^l + 1$$

for  $i = 1, 2, 3, 4$  and the two possibilities for  $(d, \mu)$ . More precisely, if  $7 \nmid z$ , then

$$\begin{aligned} \left( \frac{\gamma_1\gamma_2}{z_1^4}, \frac{\alpha_2\gamma_1^l - \alpha_3\gamma_2^l}{\alpha_1z_1^{2l}} \right) &\in C_{l,1}(K), & \left( \frac{\gamma_2z_1^2}{\gamma_1^2}, \frac{\alpha_3\gamma_2^l - \alpha_1z_1^{2l}}{\alpha_2\gamma_1^l} \right) &\in C_{l,2}(K), \\ \left( \frac{z_1^2\gamma_1}{\gamma_2^2}, \frac{\alpha_1z_1^{2l} - \alpha_2\gamma_1^l}{\alpha_3\gamma_2^l} \right) &\in C_{l,3}(K), & \left( \frac{\gamma_1\gamma_2}{\gamma_3^2}, \frac{\alpha'_1\gamma_1^l - \alpha'_2\gamma_2^l}{\alpha'_3\gamma_3^l} \right) &\in C_{l,4}(K) \end{aligned}$$

where  $C_{l,i}$  denotes the genus  $(l-1)/2$  hyperelliptic curve given by

$$C_{l,i} : Y^2 = -4\eta_i X^l + 1, \quad (\mu, d) = (1, 1), \quad i = 1, 2, 3, 4.$$

If  $7 \mid z$ , then similarly

$$\begin{aligned} \left( \frac{\gamma_1 \gamma_2}{z_1^4}, \frac{\alpha_2 \gamma_1^l - \alpha_3 \gamma_2^l}{\alpha_1 z_1^{2l}} \right) &\in D_{l,1}(K), & \left( \frac{\gamma_2 z_1^2}{\gamma_1^2}, \frac{\alpha_3 \gamma_2^l - \alpha_1 z_1^{2l}}{\alpha_2 \gamma_1^l} \right) &\in D_{l,2}(K), \\ \left( \frac{z_1^2 \gamma_1}{\gamma_2^2}, \frac{\alpha_1 z_1^{2l} - \alpha_2 \gamma_1^l}{\alpha_3 \gamma_2^l} \right) &\in D_{l,3}(K), & \left( \frac{\gamma_1 \gamma_2}{\gamma_3^2}, \frac{\alpha'_1 \gamma_1^l - \alpha'_2 \gamma_2^l}{\alpha'_3 \gamma_3^l} \right) &\in D_{l,4}(K) \end{aligned}$$

where  $D_{l,i}$  denotes the genus  $(l - 1)/2$  hyperelliptic curve given by

$$D_{l,i} : Y^2 = -4\eta_i X^l + 1, \quad (\mu, d) = (2 - \theta, 7), \quad i = 1, 2, 3, 4.$$

The possible values of  $\eta_i$  are given explicitly in Table 3. Note that if  $7 \mid z$ , then  $\eta_2 = -\eta_3$ , hence  $D_{l,2} \simeq D_{l,3}$ .

**Table 3.** Values of  $\eta_i$

$(\mu, d)$	$\eta_1$	$\eta_2$	$\eta_3$	$\eta_4$
$(1, 1)$	$2\theta^2 + \theta - 5$	$-5\theta^2 + 4\theta + 3$	$-\theta^2 - 3\theta - 2$	$\theta^2 - 3$
$(2 - \theta, 7)$	$7^4(20\theta^2 + 11\theta - 46)$	$7^{-3}(-\theta^2 + 4\theta + 3)$	$7^{-3}(\theta^2 - 4\theta - 3)$	$20\theta^2 + 11\theta - 45$

Next, we note that there must be a linear dependence between the symmetric binary quadratic forms  $(x - y)^2$ ,  $(x + y)^2$ , and  $x^2 + \theta xy + y^2$ . It is given by

$$(\theta - 2)(x - y)^2 = -4(x^2 + \theta xy + y^2) + (\theta + 2)(x + y)^2.$$

Using  $(x + y)^2 = d^{-2}z_1^{2l}$  and  $x^2 + \theta xy + y^2 = \mu\gamma^l$ , we get

$$(4.16) \quad \left( \frac{x - y}{x + y} \right)^2 = \frac{-4\mu d^2}{\theta - 2} \left( \frac{\gamma}{z_1^2} \right)^l + \frac{\theta + 2}{\theta - 2}.$$

So if  $7 \nmid z$ , then

$$(4.17) \quad \left( \frac{\gamma}{z_1^2}, \frac{x - y}{x + y} \right) \in C_{l,0}(K)$$

where  $C_{l,0}$  denotes the genus  $(l - 1)/2$  hyperelliptic curve given by

$$C_{l,0} : Y^2 = 7^{-1}(4\theta^2 + 12\theta + 16)X^l + 7^{-1}(-4\theta^2 - 12\theta - 9).$$

If  $7 \mid z$ , then

$$\left( \frac{\gamma}{z_1^2}, \frac{x - y}{x + y} \right) \in D_{l,0}(K)$$

where  $D_{l,0}$  denotes the genus  $(l - 1)/2$  hyperelliptic curve given by

$$D_{l,0} : Y^2 = 14^2 X^l + 7^{-1}(-4\theta^2 - 12\theta - 9).$$

Thus we have reduced our problem to determining the  $K$ -rational points on two genus  $(l - 1)/2$  curves: one of the  $C_{l,i}$  and one of the  $D_{l,i}$ . Note that

$$(4.18) \quad C_{l,i}(K) \supset \begin{cases} \{\infty, (1, \pm 1)\} & \text{if } i = 0, \\ \{\infty, (0, \pm 1), (1, \pm(2\theta^2 - 5))\} & \text{if } i = 1, \\ \{\infty, (0, \pm 1), (1, \pm(2\theta^2 - 2\theta - 1))\} & \text{if } i = 2, \\ \{\infty, (0, \pm 1), (1, \pm(2\theta + 3))\} & \text{if } i = 3, \\ \{\infty, (0, \pm 1), (1, \pm(2\theta^2 + 2\theta - 3))\} & \text{if } i = 4; \end{cases}$$

$$(4.19) \quad D_{l,i}(K) \supset \begin{cases} \{\infty\} & \text{if } i = 0, \\ \{\infty, (0, \pm 1)\} & \text{if } i = 1, 2, 3, \\ \{\infty, (0, \pm 1), (1, \pm(6\theta^2 + 4\theta - 13))\} & \text{if } i = 4. \end{cases}$$

LEMMA 4.12. *Let  $l \in L_7$ .*

- *If for at least one  $i \in \{0, 1, 2, 3, 4\}$  equality holds in (4.18), then there are no non-trivial primitive integer solutions to  $x^7 + y^7 = z^l$  with  $7 \nmid z$ .*
- *If for at least one  $i \in \{0, 1, 2, 3, 4\}$  equality holds in (4.19), then there are no non-trivial primitive integer solutions to  $x^7 + y^7 = z^l$  with  $7 \mid z$ .*

*Proof.* Let  $(x, y, z)$  be a non-trivial primitive integer solution to (1.3). We have seen that this gives rise to a  $P = (X, Y) \in C_{l,i}(K)$  for all  $i \in \{0, 1, 2, 3, 4\}$  if  $7 \nmid z$ , and it gives rise to a  $P = (X, Y) \in D_{l,i}(K)$  for all  $i \in \{0, 1, 2, 3, 4\}$  if  $7 \mid z$ . Obviously,  $P \neq \infty$  and  $X \neq 0$ . So the first part of the lemma (i.e. the  $7 \nmid z$  case) follows if we prove that  $X \neq 1$ , and the second part of the lemma (i.e. the  $7 \mid z$  case) follows if we prove that  $X \neq 1$  for  $i = 4$ . Let  $\gamma = \gamma_1, \gamma_2, \gamma_3, z_1$  be as before. Note that they are non-zero pairwise coprime algebraic integers in  $K = \mathbb{Q}[\theta]$  and of course  $z_1 \in \mathbb{Z}$ . Also note that the roots of unity in  $\mathbb{Z}[\theta]$  are  $\pm 1$ . For  $i = 0, 1, 2, 3, 4$  we have respectively

$$X = \frac{\gamma}{z_1^2}, \frac{\gamma_1 \gamma_2}{z_1^4}, \frac{\gamma_2 z_1^2}{\gamma_1^2}, \frac{z_1^2 \gamma_1}{\gamma_2^2}, \frac{\gamma_1 \gamma_2}{\gamma_3^2}.$$

Furthermore, recall that

$$x^2 + \theta xy + y^2 = \mu \gamma^l$$

where  $\mu = 1$  if  $7 \nmid z$ , and  $\mu = 2 - \theta$  if  $7 \mid z$ .

Let us assume that  $7 \nmid z$ . From the condition  $X = 1$  we now see that  $z_1^2 = 1$  and that the  $\gamma_i$  are units. If  $i = 0$ , then we get  $\gamma = 1$ . If  $i = 1$ , then we get  $1 = \gamma_1 \gamma_2 = \text{Norm}(\gamma)/\gamma_3 = \pm 1/\gamma_3$ , hence  $\gamma = \pm 1$ . If  $i = 2$ , then  $\gamma_2 = \gamma_1^2$ , and from the Galois action we see that  $\gamma_2^8 = \gamma_2$ , which implies  $\gamma_2 = 1$  and hence  $\gamma = 1$ . If  $i = 3$ , then similarly to the previous case we get  $\gamma = 1$ . Finally, if  $i = 4$ , then  $1 = \gamma_1 \gamma_2 / \gamma_3^2 = \text{Norm}(\gamma)/\gamma_3^3 = \pm 1/\gamma_3^3$ , which implies  $\gamma_3 = \pm 1$  and hence  $\gamma = \pm 1$ . In all cases we see that  $\gamma = \pm 1$ , so

$$x^2 + \theta xy + y^2 = \pm 1.$$

Since  $x, y, \in \mathbb{Z}$ , we get  $xy = 0$ , a contradiction which proves the first part of the lemma.

Now assume  $7 \mid z$ . We let  $i = 4$ . The condition  $X = 1$  implies, as before, that  $\gamma = \pm 1$ . This gives us

$$x^2 + \theta xy + y^2 = \pm(2 - \theta).$$

The integer solutions are  $(x, y) = (\pm 1, \mp 1)$ , hence  $z = 0$ , a contradiction which proves the second part of the lemma. ■

REMARK 4.13. We know of at least one instance where equality does not hold in (4.19), namely

$$(4.20) \quad D_{13,1}(K) \supset \{\infty, (0, \pm 1), (7^{-1}(3\theta^2 + 2\theta - 2), \pm(4\theta^2 + 6\theta + 1))\}.$$

It is of course a simple matter to check that the pair of ‘new’ points does not come from a non-trivial primitive integer solution to (1.3), from which we conclude that equality in (4.20) implies the non-existence of non-trivial primitive integer solutions to (1.3) with  $7 \mid z$  and  $l = 13$ . Although it seems very likely that indeed this equality holds, proving it still remains quite a challenge.

REMARK 4.14. Instead of finding the full set  $S$  of  $K$ -rational points on one of the  $C_{l,i}$  or  $D_{l,i}$  in order to apply Lemma 4.12, it can be convenient to use extra (local) information so that the same conclusion can be obtained by finding a specific subset of  $S$  satisfying extra (local) conditions. For example, let  $\mathfrak{P}$  be the prime above 7; then for  $j = 1, 2, 3$  we have  $x^2 + \theta_j xy + y^2 \equiv (x + y)^2 \pmod{\mathfrak{P}}$ . So for a primitive integer solution to (1.3) with  $7 \nmid z$  we deduce, using  $\gamma_1, \gamma_2, \gamma_3, z_1$  as before, that  $\gamma_1^l \equiv \gamma_2^l \equiv \gamma_3^l \equiv (z_1^2)^l \pmod{\mathfrak{P}}$ . Since  $l \neq 2, 3$  and  $7 \nmid z$ , we obtain respectively

$$(4.21) \quad \gamma_1 \equiv \gamma_2 \equiv \gamma_3 \equiv z_1^2 \pmod{\mathfrak{P}}, \quad \gamma_1 \gamma_2 \gamma_3 z_1^2 \not\equiv 0 \pmod{\mathfrak{P}}.$$

We note that  $C_{l,i}$  for  $i = 1, 2, 3, 4$  has good reduction at  $\mathfrak{P}$ . Now the local information (4.21) implies that our solution gives rise to a point  $\tilde{P}_i$  on the reduction  $\tilde{C}_{l,i}/\mathbb{F}_7$  where

$$\tilde{P}_i = (1, 3), (1, 4), (1, 0), (1, 2)$$

for  $i = 1, 2, 3, 4$  respectively. Therefore define, for  $i = 1, 2, 3, 4$ ,

$$C_{l,i}(K)' := \{P \in C_{l,i}(K) : P \pmod{\mathfrak{P}} = \tilde{P}_i\}.$$

For the curve  $C_{l,0}$  we see, by (4.17), that any  $P \in C_{l,0}(K)$  that comes from a solution to (1.3) has second coordinate in  $\mathbb{Q}$ , where by convention we say that  $\infty$  has second coordinate in  $\mathbb{Q}$ . Therefore define

$$C_{l,0}(K)' := \{P \in C_{l,0}(K) : P \text{ has second coordinate in } \mathbb{Q}\}.$$

We arrive at the following refined version of the first part of Lemma 4.12.



LEMMA 4.15. *Let  $l \in L_7$ . If for at least one  $i \in \{0, 1, 2, 3, 4\}$  we have*

$$C_{l,i}(K)' = \begin{cases} \{\infty, (1, \pm 1)\} & \text{if } i = 0, \\ \{(1, 2\theta^2 - 5)\} & \text{if } i = 1, \\ \{(1, -2\theta^2 + 2\theta + 1)\} & \text{if } i = 2, \\ \{(1, \pm(2\theta + 3))\} & \text{if } i = 3, \\ \{(1, 2\theta^2 + 2\theta - 3)\} & \text{if } i = 4, \end{cases}$$

*then there are no non-trivial primitive integer solutions to  $x^7 + y^7 = z^l$  with  $7 \nmid z$ .*

Similar remarks apply to  $D_{l,0}$  and  $D_{l,4}$ .

**4.4. Rational points on  $C_{l,i}$  and  $D_{l,i}$ .** The curves  $C_{l,i}$  for  $i = 0, \dots, 4$  and  $D_{l,4}$  contain a  $K$ -rational point  $P = (X, Y)$  with  $X = 1$ . We can check that  $D := [P - \infty]$  is a point of infinite order on the Jacobian. Upper bounds for the ranks of the Jacobians of the  $C_{5,i}$  and the  $D_{5,i}$  can be found in Tables 4 and 5 respectively. We conclude that

$$\begin{aligned} \text{rank Jac}(C_{5,1})(K) &= \text{rank Jac}(C_{5,2})(K) = \text{rank Jac}(C_{5,3})(K) = 1, \\ \text{rank Jac}(D_{5,4})(K) &= 1, \quad \text{rank Jac}(D_{5,2})(K) = 0. \end{aligned}$$

We see that we are in a good position to solve (1.3) for  $l = 5$ . For the case  $7 \nmid z$  the candidates  $C_{5,1}$ ,  $C_{5,2}$ , and  $C_{5,3}$  seem equally promising at this point; we choose to work with  $C_{5,3}$ . For the case  $7 \mid z$ , the curves  $D_{5,1}$  and  $D_{5,2}$  are both good candidates, but obviously  $D_{5,2}$  is the easier one to work with, since its Jacobian has rank zero.

**Table 4.** Rank bounds for the Jacobian of  $C_{5,i}$

$C$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(K, \text{Jac}(C))$	Time
$C_{5,0}$	2	1545 s
$C_{5,1}$	1	1667 s
$C_{5,2}$	1	1700 s
$C_{5,3}$	1	1928 s
$C_{5,4}$	2	571 s

**Table 5.** Rank bounds for the Jacobian of  $D_{5,i}$

$D$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(K, \text{Jac}(D))$	Time
$D_{5,0}$	1	79083 s $\approx$ 22.0 h
$D_{5,1}$	1	89039 s $\approx$ 24.7 h
$D_{5,2} (\simeq D_{5,3})$	0	102817 s $\approx$ 28.6 h
$D_{5,4}$	1	1838 s

PROPOSITION 4.16. *We have*

$$C_{5,3}(K)' = \{(1, \pm(2\theta + 3))\}, \quad D_{5,2}(K) = \{\infty, (0, \pm 1)\}.$$

*Proof.* We will first determine  $C_{5,3}(K)'$  and write for now  $J := \text{Jac}(C_{5,3})$ . Let  $P_{\pm} := (1, \pm(2\theta + 3)) \in C_{5,3}(K)$  and  $D := [P_+ - \infty] \in J(K)$ . Then, as remarked before,  $D$  has infinite order. Since we need this fact in the proof, we will supply details here. Using explicit computations in **MAGMA** it is straightforward to check this, but it can actually easily be shown ‘by hand’ as follows. Note that  $C_{5,3}$ , and hence  $J$ , has good reduction at the prime  $\mathfrak{P}$  above 7; denote the reductions by  $\tilde{C}_{5,3}$  and  $\tilde{J}$  respectively. The points  $P_{\pm}$  reduce to a single Weierstrass point  $\tilde{P} = (1, 0) \in \tilde{C}_{5,3}(\mathbb{F}_7)$ . Thus the reduction  $\tilde{D}$  of  $D$  has order 2 in  $\tilde{J}(\mathbb{F}_7)$ . Since the hyperelliptic polynomial  $f := -4\eta_3 X^5 + 1$  in the defining equation for  $C_{5,3}$  is irreducible, we see that  $\#J(K)_{\text{tors}}$  is odd. This implies that any elements of  $J(K)$  whose reduction modulo a prime of good reduction has even order cannot be torsion, in particular  $D$  has infinite order.

Now we will apply Chabauty–Coleman with the prime  $\mathfrak{P}$ . A basis for  $\Omega(C_{5,3}/K_{\mathfrak{P}})$  is given by  $X^i dX/Y$  with  $i = 0, 1$ . We have explicitly  $2D = [P_+ - P_-]$ , which also has infinite order of course. We note that the rational function  $X - 1$  does not reduce to a local uniformizer at  $\tilde{P}$ , but the function  $T := Y + Y_0$  does, where  $Y_0 := 2\theta + 3$ . We compute  $2Y dY = -20\eta_3 X^4 dX$ , so

$$X^i \frac{dX}{Y} = X^i \frac{dY}{-10\eta_3 X^4} = \frac{dT}{-10\eta_3 X^{4-i}}.$$

Furthermore, (with the obvious choice for the 5th root) around  $P_-$  we have

$$\begin{aligned} X^{-1} &= \left( \frac{Y^2 - 1}{-4\eta_3} \right)^{-1/5} = \left( 1 + \frac{T^2 - 2Y_0 T}{-4\eta_3} \right)^{-1/5} \\ &= 1 + \frac{-\theta + 2}{10} T + \frac{13\theta^2 - 17\theta + 2}{100} T^2 + \frac{287\theta^2 - 274\theta - 103}{1000} T^3 + \dots \in K[[T]]. \end{aligned}$$

Formal integration allows us to calculate to high enough  $\mathfrak{P}$ -adic precision

$$c_i := \int_0^{2D} X^i \frac{dX}{Y} = \int_{P_-}^{P_+} X^i \frac{dX}{Y} = \int_0^{2Y_0} \frac{dT}{-10\eta_3 X^{4-i}}.$$

We note  $v_{\mathfrak{P}}(c_0) = v_{\mathfrak{P}}(c_1) = 1$ . Now  $\omega := (-c_1/c_0 + X) dX/Y \in \text{Ann}(J(K))$  and the function

$$f(T) := \int_0^T \frac{(-c_1/c_0 + X(T')) dT'}{-10\eta_3 X(T')^4}$$

vanishes for  $T \in Y_0 \mathcal{O}_{K_{\mathfrak{P}}}$  such that  $(X(T), Y(T)) \in C_{5,3}(K)$ , which have to reduce mod  $\mathfrak{P}$  to  $\tilde{P}$ . The Strassmann bound for the power series in  $t$  of

$f(Y_0t)$  can be computed to be 3. The zeroes  $t = 0$  and  $t = 2$  correspond to the points  $P_-$  and  $P_+$  respectively. The third solution occurs at  $t = 1$ , which corresponds to the unique Hensel lift of  $\tilde{P}$  to a  $\mathfrak{P}$ -adic Weierstrass point. This last point is not  $K$ -rational (since  $f$  is irreducible over  $K$ ), so we conclude that  $C_{5,3}(K)' = \{P_{\pm}\}$ . Further details can be found in our MAGMA script `Chabauty771.m`.

Determining  $D_{5,2}(K)$  is straightforward, since  $J := \text{Jac}(D_{5,2})$  has rank 0. The number of points on the reduction of  $J$  at the prime above  $p$  for  $p = 3, 11$  can be calculated to equal 730 and 1882705 respectively. Their gcd equals 5. Since  $[(0, 1) - \infty] \in J(K)$  is non-trivial, it must be a point of order 5 generating  $J(K)$ . The Abel–Jacobi map

$$D_{5,2}(K) \rightarrow J(K), \quad P \mapsto [P - \infty],$$

is injective. The points  $n[(0, 1) - \infty]$  for  $n = 2, 3$  cannot be represented as  $[P - \infty]$  for some  $P \in D_{5,2}(K)$ . This shows that  $D_{5,2}(K) = \{\infty, (0, \pm 1)\}$ . ■

Obviously, the proposition above together with Lemmata 4.12 and 4.15 implies Theorem 2.

REMARK 4.17. With a bit more work it is possible to determine  $C_{5,3}(K)$  completely, as well as  $C_{5,1}(K)$ ,  $C_{5,2}(K)$ , and  $D_{5,4}(K)$ . In an earlier version of this paper we only dealt with the curves  $C_{5,4}$  and  $D_{5,4}$ , so we had to determine  $C_{5,4}(K)$  as well. For this curve it is in fact possible to find another independent  $K$ -rational point on the Jacobian and use Chabauty over number fields [21] to determine  $C_{5,4}(K)$  on this genus 2 curve of rank 2 over  $K$ .

**5. Results assuming GRH.** The purpose of this section is to prove Theorem 3. There are however many other, unconditional, results in this section, which can be interesting in their own right. When a result is conditional on GRH, we shall clearly state so. We shall start with the equation  $x^7 + y^7 = z^l$ , since the treatment is a direct continuation of the previous section. After this, the equation  $x^5 + y^5 = z^l$  will be revisited. In the final section we shall briefly discuss the possibility of making the results unconditional.

**5.1. The equation  $x^7 + y^7 = z^l$  for  $l = 11, 13$ .** As in the  $l = 5$  case, we can check that for  $l \in \{11, 13\}$  the  $K$ -rational points on  $C_{l,i}$  for  $i = 0, 1, 2, 3, 4$  and  $D_{l,4}$  give rise to a point of infinite order on their Jacobians. Assume GRH. Rank bounds for the Jacobians of the  $C_{l,i}$  and the  $D_{l,i}$  with  $l \in \{11, 13\}$  can be found in Tables 6 and 7 respectively. We want to stress again that because of the pseudo-random number generator involved in computing the ranks, the computation time also depends (really heavily this time) on the seed. We conclude from the tables that

$$\text{rank Jac}(C_{11,3})(K) = 1, \quad \text{rank Jac}(D_{11,4})(K) = 1,$$

and of course

$$\text{rank Jac}(D_{11,0})(K) = 0, \quad \text{rank Jac}(D_{13,2})(K) = 0.$$

**Table 6.** (GRH) Rank bounds for the Jacobian of  $C_{l,i}$

$C$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(K, \text{Jac}(C))$	Time
$C_{11,0}$	4	10481 s $\approx$ 2.9 h
$C_{11,1}$	3	4226 s $\approx$ 1.2 h
$C_{11,2}$	2	7207 s $\approx$ 2.0 h
$C_{11,3}$	1	3604 s $\approx$ 1.0 h
$C_{11,4}$	2	14816 s $\approx$ 4.1 h
$C_{13,0}$	2	10508 s $\approx$ 2.9 h
$C_{13,1}$	2	365096 s $\approx$ 4.2 days
$C_{13,2}$	2	108629 s $\approx$ 30.2 h
$C_{13,3}$	4	107770 s $\approx$ 29.9 h
$C_{13,4}$	3	119062 s $\approx$ 33.1 h

**Table 7.** (GRH) Rank bounds for the Jacobian of  $D_{l,i}$

$D$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(K, \text{Jac}(D))$	Time
$D_{11,0}$	0	6419 s $\approx$ 1.8 h
$D_{11,1}$	1	7550 s $\approx$ 2.1 h
$D_{11,2} (\simeq D_{11,3})$	2	12010 s $\approx$ 3.3 h
$D_{11,4}$	1	1800 s $\approx$ 0.5 h
$D_{13,0}$	2	469263 s $\approx$ 5.4 days
$D_{13,1}$	3	91258 s $\approx$ 25.3 h
$D_{13,2} (\simeq D_{13,3})$	0	43182 s $\approx$ 12.0 h
$D_{13,4}$	3	10225 s $\approx$ 2.8 h

We see that we are in a good position to solve (1.3) for  $l = 11$ , but that we have insufficient information to treat the  $7 \nmid z$  case when  $l = 13$ .

PROPOSITION 5.1. *Assuming GRH, we have*

$$C_{11,3}(K)' = \{(1, \pm(2\theta + 3))\}, \quad D_{11,0}(K) = \{\infty\}.$$

*Proof.* The proof that  $C_{11,3}(K)' = \{(1, \pm(2\theta + 3))\}$  is analogous to our proof that  $C_{5,3}(K)' = \{(1, \pm(2\theta + 3))\}$  given in Proposition 4.16. Details can be found in our MAGMA script `Chabauty771.m`.

Since  $\text{rank Jac}(D_{11,0})(K) = 0$  we can get  $D_{11,0}(K) = \{\infty\}$  from the fact that  $\text{Jac}(D_{11,0})(K)_{\text{tors}}$  is trivial. This last statement follows from observing that the defining equation for  $D_{11,0}$  shows that  $\# \text{Jac}(D_{11,0})(K)_{\text{tors}}$  is odd

and counting points on the reduction of  $\text{Jac}(D_{11,0})$  modulo the prime above 5 and a prime above 13. ■

**COROLLARY 5.2.** *Assuming GRH, there are no non-trivial primitive integer solutions to (1.3) for  $l = 11$ .*

**5.2. The equation  $x^5 + y^5 = z^l$  revisited.** Instead of just working over  $\mathbb{Q}$ , like we did in Section 3, we shall use the factorization of  $H_p$  over  $\mathbb{Q}(\zeta_p)$  and  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ , like we did in Section 4, but now with  $p = 5$  instead of  $p = 7$  of course.

**5.2.1. Initial factorizations for  $x^5 + y^5 = z^l$ .** Let  $(x, y, z)$  be a primitive integer solution to (1.2) with  $5 \nmid z$  for some prime  $l > 5$ . Recall that

$$H_5(x, y) = \frac{x^5 + y^5}{x + y} = x^4 - x^3y + x^2y^2 - xy^3 + y^4.$$

By Lemma 2.2,  $\gcd(x + y, H_5(x, y)) = 1$ , and consequently

$$x + y = z_1^l, \quad H_5(x, y) = z_2^l, \quad z = z_1 z_2$$

where  $z_1, z_2$  are non-zero, coprime integers.

Let  $\zeta$  denote a primitive 5th root of unity,  $L = \mathbb{Q}(\zeta)$  and  $\mathcal{O} = \mathbb{Z}[\zeta]$  be the ring of integers of  $L$ . The class number of  $\mathcal{O}$  is 1 and the unit rank is 1. The unit group is in fact

$$\{\pm \zeta^i (1 + \zeta)^r : 0 \leq i \leq 4, r \in \mathbb{Z}\}.$$

Moreover, 5 ramifies as  $5\mathcal{O} = (1 - \zeta)^4 \mathcal{O}$ . Now  $H_5(x, y) = \text{Norm}(x + \zeta y)$ . We have

$$(5.1) \quad x + \zeta y = (1 + \zeta)^r \beta^l, \quad 0 \leq r \leq l - 1,$$

for some  $\beta \in \mathbb{Z}[\zeta]$ . Thus we have  $l$  cases to consider. Using a modular approach, we can reduce the number of cases to just 1 for many values of  $l$ , e.g.  $l = 11, 13, 17$ .

**5.2.2. A modular approach to  $x^5 + y^5 = z^l$  when  $5 \nmid z$ .** Consider the set

$$L_5 := \{\text{primes } l : 5 < l < 100\}.$$

**PROPOSITION 5.3.** *Let  $(x, y, z)$  be a primitive integer solution to (1.2) with  $5 \nmid z$  and  $l \in L_5$ . Then (5.1) holds with  $r = 0$ .*

The proof is very much analogous to that of Proposition 4.1. So we just describe the main steps. We use the Frey curve

$$E_{x,y} : Y^2 = X^3 - 5(x^2 + y^2)X^2 + 5H_5(x, y)X.$$

Write  $\rho_l^{x,y}$  for the Galois representation on the  $l$ -torsion of  $E_{x,y}$ . Since  $E_{x,y}$  is a quadratic twist of the Frey curve from Section 3.2 (which is also denoted as  $E_{x,y}$  there), the irreducibility of  $\rho_l^{x,y}$  for primes  $l \geq 7$  follows directly from Lemma 3.7. Now a straightforward computation of the conductor and

minimal discriminant of  $E_{x,y}$ , and an application of modularity [3] and level lowering [19], [20] as usual, yield the following lemma.

LEMMA 5.4. *For a prime  $l \geq 7$ , the Galois representation  $\rho_l^{x,y}$  arises from a newform  $f$  of level  $N = 2^\alpha 5^2$  where  $\alpha = 1, 3$ , or  $4$ .*

There are respectively 2, 5, and 8 newforms at these levels, which all happen to be rational. Specializing  $E_{x,y}$  at a trivial primitive integer solution with  $xy = 0$  (i.e.  $(x, y) = (\pm 1, 0)$  or  $(0, \pm 1)$ ) yields  $E_{200b_1}$ , and specializing at  $(x, y) = (\pm 1, \pm 1)$  (which does not correspond to a solution) yields  $E_{400d_2}$ . Note that in the latter case we have  $H_5(x, y) = 1$ . By comparing traces of Frobenius as usual (including the method of Kraus for some small values of  $l$ ), we can eliminate all but two of the 15 newforms for all primes  $l \geq 7$ . The two exceptions are of course the two newforms corresponding to the two elliptic curves we just obtained by specialization of  $E_{x,y}$ . We note that in the case  $p|z$  it is convenient to strengthen  $a_p(E_0) \equiv \pm(1+p) \pmod{l}$  to  $a_p(E_0) \equiv a_p(E_{x,y})(1+p) \pmod{l}$ .

LEMMA 5.5. *For a prime  $l \geq 7$ , the Galois representation  $\rho_l^{x,y}$  arises from either  $E_{200b}$  or  $E_{400d}$ .*

By a basic application of Kraus' method we are able to eliminate the possibility of  $E_{400d}$  for all  $l \in L_5$  except  $l = 7, 11, 19$ . These remaining three cases can be dealt with using an analogue of Lemma 4.10.

LEMMA 5.6. *For  $l \in L_5$ , the Galois representation  $\rho_l^{x,y}$  does not arise from  $E_{400d}$ .*

To finish the proof of Proposition 5.3 we now only have to deal with  $E_{200b}$ , which is possible using again the analogue of Lemma 4.10. Computational details can be found in the second part of the MAGMA script `Modular551.m`.

**5.2.3. The hyperelliptic curves.** Let  $\theta = \zeta + \zeta^{-1}$  and  $K = \mathbb{Q}(\theta)$ ; this is the totally real quadratic subfield of  $L$ . The Galois conjugates of  $\theta$  are  $\theta_1, \theta_2$ , which in terms of  $\zeta$  are given by

$$\theta_1 = \zeta + \zeta^{-1}, \quad \theta_2 = \zeta^2 + \zeta^{-2}.$$

Note that

$$\theta_1 = \theta, \quad \theta_2 = -1 - \theta.$$

Let

$$\gamma = \text{Norm}_{L/K}(\beta).$$

Taking norms in (5.1) with  $r = 0$  down to  $K$  we obtain

$$x^2 + \theta xy + y^2 = \gamma^l.$$

Let  $\gamma_1 = \gamma$  and  $\gamma_2$  denote the conjugates of  $\gamma$  that correspond respectively to  $\theta \mapsto \theta_j$  for  $j = 1, 2$ . Then

$$x^2 + \theta_1 xy + y^2 = \gamma_1^l, \quad x^2 + \theta_2 xy + y^2 = \gamma_2^l.$$

Furthermore, recall that

$$(x + y)^2 = z_1^{2l}.$$

The left-hand sides of the previous three equations are symmetric binary quadratic forms over  $K$ , hence linearly dependent. We calculate

$$(x + y)^2 + \theta_2(x^2 + \theta_1xy + y^2) + \theta_1(x^2 + \theta_2xy + y^2) = 0.$$

In terms of the coordinates  $z_1^2, \gamma_1, \gamma_2$  we get

$$z_1^{2l} + \theta_2\gamma_1^l + \theta_1\gamma_2^l = 0.$$

Using Remark 4.11, we see that

$$\left( \frac{z_1^2\gamma_1}{\gamma_2^2}, \frac{z_1^{2l} - \theta_2\gamma_1^l}{\theta_1\gamma_2^l} \right) \in C_{l,1}(K)$$

where  $C_{l,1}$  is the genus  $(l-1)/2$  hyperelliptic curve given by

$$(5.2) \quad C_{l,1} : Y^2 = -4\eta_1 X^l + 1, \quad \eta_1 = \theta_2/\theta_1^2 = -2\theta - 3.$$

The linear dependence between the symmetric binary quadratic forms  $(x-y)^2$ ,  $(x+y)^2$ , and  $x^2 + \theta xy + y^2$  is given by

$$(\theta - 2)(x - y)^2 = -4(x^2 + \theta xy + y^2) + (\theta + 2)(x + y)^2.$$

Using  $(x + y)^2 = z_1^{2l}$  and  $x^2 + \theta xy + y^2 = \gamma^l$ , we get

$$(5.3) \quad \left( \frac{x - y}{x + y} \right)^2 = \frac{-4}{(\theta - 2)} \left( \frac{\gamma}{z_1^2} \right)^l + \frac{\theta + 2}{\theta - 2}.$$

We compute  $-4/(\theta - 2) = 4(\theta + 3)/5$  and  $(\theta + 2)/(\theta - 2) = -(4\theta + 7)/5$ . Hence

$$P := \left( \frac{\gamma}{z_1^2}, \frac{x - y}{x + y} \right) \in C_{l,0}(K)$$

where  $C_{l,0}$  is the genus  $(l-1)/2$  hyperelliptic curve given by

$$(5.4) \quad C_{l,0} : 5Y^2 = (4\theta + 12)X^l - (4\theta + 7).$$

Note that in fact the second coordinate of  $P$  lies in  $\mathbb{Q}$ . Furthermore, since 5 is a square in  $K$ , the factor 5 in front of  $Y^2$  above could easily be absorbed by rescaling  $Y$  (by a factor of  $2\theta + 1$ ). However, this would spoil the nice feature of the curve that the points of our interest have second coordinate lying in  $\mathbb{Q}$ .

Regarding  $K$ -rational points on the curves  $C_{l,0}$  and  $C_{l,1}$ , we note that

$$(5.5) \quad C_{l,i}(K) \supset \begin{cases} \{\infty, (1, \pm 1)\} & \text{if } i = 0, \\ \{\infty, (0, \pm 1), (1, \pm \eta_1)\} & \text{if } i = 1. \end{cases}$$

As in (the first part of) Lemma 4.12, we have the following.

LEMMA 5.7. *Let  $l \in L_5$ . If for  $i = 0$  or  $i = 1$  equality holds in (5.5), then there are no non-trivial primitive integer solutions to  $x^5 + y^5 = z^l$  with  $5 \nmid z$ .*

Let  $\mathfrak{P}$  be the prime above 5. We note that  $C_{l,1}$  has good reduction at  $\mathfrak{P}$ . Define

$$C_{l,1}(K)' := \{P \in C_{l,i}(K) : P \pmod{\mathfrak{P}} = (1, 2)\}.$$

As in the  $x^7 + y^7 = z^l$  case, define as well

$$C_{l,0}(K)' := \{P \in C_{l,0}(K) : P \text{ has second coordinate in } \mathbb{Q}\}.$$

Completely similarly to Remark 4.14, we arrive at a refinement of Lemma 5.7.

LEMMA 5.8. *Let  $l \in L_5$ . If for  $i = 0$  or  $i = 1$  we have*

$$C_{l,i}(K)' = \begin{cases} \{\infty, (1, \pm 1)\} & \text{if } i = 0, \\ \{(1, 2\theta + 3)\} & \text{if } i = 1, \end{cases}$$

*then there are no non-trivial primitive integer solutions to  $x^5 + y^5 = z^l$  with  $5 \nmid z$ .*

**5.2.4. Rational points on  $C_{l,i}$ .** For  $i = 0, 1$  let  $J_{l,i} := \text{Jac}(C_{l,i})$ . For  $l = 11, 13, 17$  it is easy to check that

$$[(1, 1) - \infty] \in J_{l,0}(K), \quad [(1, \eta_1) - \infty] \in J_{l,1}(K)$$

are points of infinite order. Assume GRH. For these values of  $l$  we also computed upper bounds for the ranks of  $J_{l,0}(K)$  and  $J_{l,1}(K)$ ; see Table 8.

**Table 8.** (GRH) Rank bounds for the Jacobians of  $C_{l,0}$  and  $C_{l,1}$

$l$	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(K, \text{Jac}(C_{l,0}))$	Time	$\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(K, \text{Jac}(C_{l,1}))$	Time
11	1	55 s	2	145 s
13	2	178 s	1	175 s
17	4	2178 s	2	13087 s

We conclude that  $J_{11,0}(K)$  and  $J_{13,1}(K)$  both have rank 1 and that there is an explicit generator for a finite index subgroup for both of them. Hence, we are again in a position to apply Chabauty–Coleman.

LEMMA 5.9. *Assuming GRH, we have*

$$\begin{aligned} C_{11,0}(K)' &= \{\infty, (1, \pm 1)\}, \\ C_{13,1}(K)' &= \{(1, 2\theta + 3)\}. \end{aligned}$$

*Proof.* We start by determining  $C_{11,0}(K)'$  using Chabauty–Coleman with the prime  $\mathfrak{P}$  above 3. The curve  $C_{11,0}$  has good reduction at  $\mathfrak{P}$ . This reduction, denoted  $\tilde{C}_{11,0}$ , contains ten  $\mathbb{F}_9$ -rational points, but the subset of  $\mathbb{F}_9$ -rational points whose second coordinate is  $\mathbb{F}_3$ -rational consists only of the four points  $\infty, (1, \pm 1), (\tilde{X}_0, 0)$  where  $\tilde{X}_0 \in \mathbb{F}_9$  with  $\tilde{X}_0^2 = -1$ . If we show that for each  $\tilde{P} = \infty, (1, \pm 1)$  we have a unique lift to  $P \in C_{11,0}(K)$



and that  $(\tilde{X}_0, 0)$  does not lift to a point in  $C_{11,0}(K)$  it will then follow that  $C_{11,0}(K)' = \{\infty, (1, \pm 1)\}$ .

A basis for  $\Omega(C_{11,0}/K_{\mathfrak{P}})$  is given by  $X^i dX/Y$  for  $i = 0, 1, \dots, 4$ . We can compute

$$c_i := \int_0^D X^i \frac{dX}{Y}, \quad i = 0, 1, \dots, 4,$$

to high enough  $\mathfrak{P}$ -adic precision and find e.g.  $v_{\mathfrak{P}}(c_2) = v_{\mathfrak{P}}(c_4) = v_{\mathfrak{P}}(c_4 - c_2) = v_{\mathfrak{P}}(c_4 + c_2) = 1$ . Write  $u := -c_2/c_4$  and let  $\omega := (X^2 + uX^4)dX/Y$ . Then we see that  $\omega \in \text{Ann}(\text{Jac}(C_{11,0})(K))$  and it reduces to a differential  $\tilde{\omega}$  on  $\tilde{C}_{11,0}/\mathbb{F}_9$ . Since  $v_{\mathfrak{P}}(u) = v_{\mathfrak{P}}(c_2) - v_{\mathfrak{P}}(c_4) = 0$ , we see that  $\tilde{\omega}$  does not vanish at  $\infty$ . Similarly, since  $v_{\mathfrak{P}}(1 + u) = v_{\mathfrak{P}}(c_4 - c_2) - v_{\mathfrak{P}}(c_4) = 0$ , we see that  $\tilde{\omega}$  does not vanish at  $(1, \pm 1)$ . Finally, since  $v_{\mathfrak{P}}(-1 + u) = v_{\mathfrak{P}}(c_4 + c_2) - v_{\mathfrak{P}}(c_4) = 0$ , we see that  $\tilde{\omega}$  does not vanish at  $(\tilde{X}_0, 0)$ . Consequently, for each  $\tilde{P} = \infty, (1, \pm 1)$  we have a unique lift to  $P \in C_{11,0}(K)$ . The point  $(\tilde{X}_0, 0)$  Hensel-lifts uniquely to a Weierstrass point  $(X_0, 0) \in C_{11,0}(K_p)$ , which is not  $K$ -rational. This finishes the first part of the reasoning, as in the proof of Proposition 3.2.

Next we determine  $C_{13,1}(K)'$  using Chabauty–Coleman with the prime  $\mathfrak{P}$  above 5. The curve  $C_{13,1}$  has good reduction at  $\mathfrak{P}$ , denoted  $\tilde{C}_{13,1}$ . Let  $T = X - 1$  be a uniformizer at  $P = (1, 2\theta + 3)$ . A basis for  $\Omega(C_{13,1}/K_{\mathfrak{P}})$  is given by  $T^i dT/Y$  for  $i = 0, 1, \dots, 5$ . We can compute

$$c_i := \int_0^D T^i \frac{dT}{Y}, \quad i = 0, 1, \dots, 5,$$

to high enough  $\mathfrak{P}$ -adic precision and find that  $v_{\mathfrak{P}}(c_0) = 1$  and  $v_{\mathfrak{P}}(c_i) = 2$  for  $i = 1, \dots, 5$ . Therefore it is impossible to find an  $\omega \in \text{Ann}(\text{Jac}(C_{13,1})(K))$  with good reduction at  $\mathfrak{P}$  which is non-vanishing at  $\tilde{P} \in \tilde{C}_{13,1}(\mathbb{F}_5)$ . Let us define instead  $\omega := (T - c_1/c_5 T^5)dT/Y$ . Then  $\omega \in \text{Ann}(\text{Jac}(C_{13,1})(K))$  and the reduction mod  $\mathfrak{P}$  has vanishing order 1 at  $\tilde{P}$ . One can indeed check that the Strassmann bound for the function

$$t \mapsto \int_0^{\pi t} \left( T - \frac{c_1}{c_5} T^5 \right) \frac{dT}{Y}$$

(with  $\pi$  a suitable uniformizing parameter) equals 2. By construction it has a double zero at  $t = 0$ , hence the only lift of  $\tilde{P}$  to  $C_{13,1}(K)$  is  $P$ . This means  $C_{13,1}(K)' = \{(1, 2\theta + 3)\}$ . Further details can be found in our MAGMA script `Chabauty551.m`. ■

We note that it should not be much harder to determine  $C_{11,0}(K)$  and  $C_{13,1}(K)$  completely. But since it is not necessary for our purposes, we will not pursue this.

**COROLLARY 5.10.** *Under GRH, there are no non-trivial primitive integer solutions to (1.2) for  $l \in \{11, 13\}$ .*

**5.3. Making the results unconditional.** Full GRH is of course not necessary, we ‘only’ need to obtain certain class and unit group information unconditionally in order to carry out 2-descent on the four Jacobians involved. For a hyperelliptic curve defined over a number field  $K$  given by an equation of the form  $y^2 = f(x)$  where  $f(x) \in K[x]$  is irreducible over  $K$ , it suffices to have available the class and unit group information for the number field  $L := K[x]/f(x)$  (or possibly only certain relative information for the extension  $L/K$ ). For example in the case of  $x^5 + y^5 = z^l$  with  $l \in \{11, 13\}$  the field  $L = L_l$  coming from the curve  $C_{11,0}$  for  $l = 11$  and  $C_{13,1}$  for  $l = 13$  is given by  $L_l = \mathbb{Q}[t]/g_l(t)$  with  $g_{11}(t) := t^{22} + 2t^{11} - 4$  and  $g_{13}(t) = t^{26} + 22t^{13} - 4$ . Assuming GRH, either MAGMA or PARI/GP can compute the class and unit group information for these two fields rather quickly. In particular, we find that the class group is trivial for both fields (assuming of course GRH). It suffices in fact to know that our conditional unit group is a finite index 2-saturated subgroup of the (unconditional) unit group. This will be easy to check and reduces the problem to verifying that the class groups of the fields  $L_{11}$  and  $L_{13}$  are trivial. This is something that can be parallelized and apparently the class group verification for at least  $L_{11}$  and probably also for  $L_{13}$  is within the reach of current technology (but the actual verification, especially for  $L_{13}$ , would in practice of course take considerable effort, time, and computer power). For  $x^7 + y^7 = z^{11}$  we are looking at number fields of (absolute) degree 33, and verifying class group information is probably not doable in practice at the moment. The case where  $7 \mid z$  might actually be solved using a Hilbert modular approach. We did not pursue this, however, since we are not able to treat the case  $7 \nmid z$  unconditionally anyway.

Alternatively, we might be able to use partial results on BSD for abelian varieties over number fields. The four Jacobians  $J$  involved, for which we need to determine the rank unconditionally, all have CM (over a cyclotomic extension) and are defined over a totally real number field. For such abelian varieties, the partial BSD result ‘if analytic rank  $\leq 1$ , then analytic rank = algebraic rank’ seems within reach; see e.g. [29]. If on top of this, we are able to compute  $L_J(1)$  in the rank 0 case and  $L'_J(1)$  in the three rank 1 cases to high enough precision to conclude that these four values are non-zero, then we have made our results unconditional. However, the computations of  $L_J(1)$  and  $L'_J(1)$  do not seem to be easier than the class group computations at the moment.

**Acknowledgments.** The authors would like to thank the anonymous referee for providing various useful comments, and Karim Belabas for dis-

cussing class group computations in PARI/GP. The first-named author was supported by a VENI grant from the Netherlands Organisation for Scientific Research (NWO). The second-named author was supported by an EPSRC Leadership Fellowship.

## References

- [1] M. A. Bennett, I. Chen, S. R. Dahmen and S. Yazdani, *Generalized Fermat equations: a miscellany*, preprint.
- [2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. 24 (1997), 235–265 (see also <http://magma.maths.usyd.edu.au/magma/>).
- [3] 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 (2001), 843–939.
- [4] N. Bruin and M. Stoll, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. 13 (2010), 272–306.
- [5] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra 322 (2009), 638–656.
- [6] H. Cohen, *Number Theory, Vol. II: Analytic and Modern Tools*, Grad. Texts in Math. 240, Springer, New York, 2007.
- [7] R. F. Coleman, *Effective Chabauty*, Duke Math. J. 52 (1985), 765–770.
- [8] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, Ph.D. thesis, Utrecht Univ., 2008.
- [9] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada 19 (1997), 3–14, 64.
- [10] H. Darmon and A. Granville, *On the equations  $z^m = F(x, y)$  and  $Ax^p + By^q = Cz^r$* , Bull. London Math. Soc. 27 (1995), 513–543.
- [11] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat’s Last Theorem*, J. Reine Angew. Math. 490 (1997), 81–100.
- [12] J. Edwards, *A complete solution to  $X^2 + Y^3 + Z^5 = 0$* , J. Reine Angew. Math. 571 (2004), 213–236.
- [13] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. 69 (1990), 353–385.
- [14] A. Kraus, *On the equation  $x^p + y^q = z^r$ : a survey*, Ramanujan J. 3 (1999), 315–333.
- [15] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, in: Explicit Methods in Number Theory. Rational Points and Diophantine Equations, Panor. Synthèses 36, Soc. Math. France, Paris, 2012, 99–117.
- [16] B. Poonen, *Some Diophantine equations of the form  $x^n + y^n = z^m$* , Acta Arith. 86 (1998), 193–205.
- [17] B. Poonen, E. F. Schaefer and M. Stoll, *Twists of  $X(7)$  and primitive solutions to  $x^2 + y^3 = z^7$* , Duke Math. J. 137 (2007), 103–158.
- [18] B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. (2) 150 (1999), 1109–1149.
- [19] K. Ribet, *On modular representations of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  arising from modular forms*, Invent. Math. 100 (1990), 431–476.
- [20] K. Ribet, *Report on mod  $l$  representations of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , in: Motives, Proc. Sympos. Pure Math. 55, part 2, Amer. Math. Soc., Providence, RI, 1994, 639–676.

- [21] S. Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory 7 (2013), 765–793.
- [22] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.
- [23] W. Stein, *Modular Forms. A Computational Approach*, Grad. Stud. Math. 79, Amer. Math. Soc., Providence, RI, 2007.
- [24] M. Stoll, *On the arithmetic of the curves  $y^2 = x^l + A$  and their Jacobians*, J. Reine Angew. Math. 501 (1998), 171–189.
- [25] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. 98 (2001), 245–277.
- [26] M. Stoll, *On the arithmetic of the curves  $y^2 = x^l + A$ , II*, J. Number Theory 93 (2002), 183–206.
- [27] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, Univ. of California at Berkeley, 1997.
- [28] A. Wiles, *Modular elliptic curves and Fermat’s Last Theorem*, Ann. of Math. (2) 141 (1995), 443–551.
- [29] S.-W. Zhang, *Gross–Zagier formula for  $GL(2)$ . II*, in: Heegner Points and Rankin L-series, Math. Sci. Res. Inst. Publ. 49, Cambridge Univ. Press, Cambridge, 2004, 191–214.

Sander R. Dahmen  
Department of Mathematics  
VU University Amsterdam  
De Boelelaan 1081a  
1081 HV Amsterdam, The Netherlands  
E-mail: s.r.dahmen@vu.nl

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

*Received on 15.9.2013  
and in revised form on 25.1.2014*

(7592)