Math. Proc. Camb. Phil. Soc. (2015), **158**, 305–329 © *Cambridge Philosophical Society* 2015
doi:10.1017/S0305004114000681
First published online 8 January 2015

Shifted powers in binary recurrence sequences

BY MICHAEL A. BENNETT†
Department of Mathematics, University of British Columbia, Vancouver, B.C., Canada.
e-mail: bennett@math.ubc.ca

SANDER R. DAHMEN‡
Department of Mathematics, VU University Amsterdam, Amsterdam, The Netherlands.
e-mail: s.r.dahmen@vu.nl

MAURICE MIGNOTTE
Department of Mathematics, University of Strasbourg, Strasbourg, France.
e-mail: mignotte@math.u-strasbg.fr

AND SAMIR SIKSEK§
Mathematics Institute, University of Warwick, Coventry.
e-mail: S.Siksek@warwick.ac.uk

(*Received* 11 *August* 2014; *revised* 10 *November* 2014)

Abstract

Let $\{u_k\}$ be a Lucas sequence. A standard technique for determining the perfect powers in the sequence $\{u_k\}$ combines bounds coming from linear forms in logarithms with local information obtained via Frey curves and modularity. The key to this approach is the fact that the equation $u_k = x^n$ can be translated into a ternary equation of the form $ay^2 = bx^{2n} + c$ (with $a, b, c \in \mathbb{Z}$) for which Frey curves are available. In this paper we consider shifted powers in Lucas sequences, and consequently equations of the form $u_k = x^n + c$ which do not typically correspond to ternary equations with rational unknowns. However, they do, under certain hypotheses, lead to ternary equations with unknowns in totally real fields, allowing us to employ Frey curves over those fields instead of Frey curves defined over $\mathbb{Q}$. We illustrate this approach by showing that the quaternary Diophantine equation $x^{2n} \pm 6x^n + 1 = 8y^2$ has no solutions in positive integers x, y, n with $x, n > 1$.

1. *Introduction*

In [**17**], Stewart proved an effective finiteness result for shifted perfect powers in binary recurrence sequences. That is, if $\{u_k\}$ is a binary recurrence sequence for which the equation

$$x^n + c = u_k \tag{1·1}$$

† Supported by NSERC.
‡ Supported by NWO.
§ Supported by an EPSRC Leadership Fellowship EP/G007268/1, and EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

has a solution in integers x, n, c and k, with $n \geqslant 2$ and $|x| > 1$, then, under mild conditions, $\max\{|x|, n\}$ is bounded above effectively in terms of c and the recurrence. This statement is actually a consequence of the following more general theorem of Shorey and Stewart [**16**].

THEOREM 1 (Shorey and Stewart). *Let a, b, c, d, e and f be integers with*

$$(b^2 - 4ac)(4acf + bde - ae^2 - cd^2 - fb^2) \neq 0.$$

If x, y and n are integers with $|x| > 1$ and $n > 2$, satisfying

$$ax^{2n} + bx^n y + cy^2 + dx^n + ey + f = 0, \tag{1·2}$$

then the maximum of $|x|, |y|$ and n is less than a number which is effectively computable in terms of a, b, c, d, e and f. Further, if $e^2 \neq 4cf$ and x and y are integers satisfying

$$ax^4 + bx^2 y + cy^2 + dx^2 + ey + f = 0,$$

then the maximum of $|x|$ and $|y|$ is less than a number which is effectively computable in terms of a, b, c, d, e and f.

To translate such effective statements to explicit ones regarding equations of the shape (1·1) or (1·2) has proven, with current technology, to be a rather challenging problem (and has been accomplished in only a handful of cases – notably in the determination of perfect powers in the Fibonacci sequence [**5**]). In this paper, we will develop a method which allows us to explicitly find all shifted perfect powers in a number of classes of Lucas recurrence sequences which are apparently inaccessible to existing techniques in the literature. Our approach combines lower bounds for linear forms in logarithms (which underlie the proof of Theorem 1) with new ideas utilising connections between Hilbert modular forms and elliptic curves defined over totally real fields.

Whilst we will develop techniques that allow one to carry out such a program in some generality, to focus our exposition we will essentially concentrate on a single example of an equation of the shape (1·2), proving the following.

THEOREM 2. *The Diophantine equation*

$$x^{2n} \pm 6x^n + 1 = 8y^2 \tag{1·3}$$

has no solutions in positive integers x, n and y, with $x, n > 1$.

This result is the final ingredient required in work of the first author [**1**] on integral points on congruent number curves. For equation (1·3), it is a fairly routine matter to obtain an absolute bound on n (via Theorem 1 or otherwise), thereby reducing the problem to that of finding the integral points on a finite collection of hyperelliptic curves. What is much less routine is the approach we take to reduce this bound. Indeed, whilst the problem of determining Fibonacci perfect powers reduces immediately to that of solving ternary equations of the shape

$$x^2 - 5y^{2n} = \pm 4, \tag{1·4}$$

for which Frey (or, if you will, Frey–Hellegouarch) curves are immediately available, the fundamental difficulty one encounters in attempting to solve equation (1·3) is that it is *a priori* quaternary rather than ternary. The principal novelty of this paper is that we are able to replace (1·3) with an equivalent ternary equation over a real quadratic field for which we are able to construct Frey curves which we can, in turn, associate with certain Hilbert modular

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

forms. As in the work of Bugeaud, Mignotte and Siksek [**5**], we obtain local information from these Frey curves to reduce our problem from one of linear forms in three logarithms, to (the computationally more efficient) two logarithms, and subsequently, to find exceptionally strong lower bounds upon $|x|$ for nontrivial solutions to (1·3), eventually contradicting more general lower bounds for linear forms in (many) complex logarithms.

2. *Recurrence sequences : descent to a ternary equation*

To begin the proof of Theorem 2, let us observe that, if $n = 2$, equation (1·3) with a $(-)$ sign is insoluble modulo 8; with a $(+)$ sign (1·3) defines a genus 1 curve that is birational over $\mathbb{Q}$ to the rank 0 elliptic curve with Cremona reference `32a1`, and one verifies that the only solutions on our affine model satisfy $(|x|, |y|) = (1, 1)$. We may thus suppose that $n > 2$ is odd and hence consider the equation

$$x^{2p} + 6x^p + 1 = 8y^2, \tag{2·1}$$

where p is an odd prime, and x and y are integers. Note that if we have

$$u^2 + 6u + 1 = 8y^2,$$

where $\eta = \mathrm{sgn}(u) \in \{-1, 1\}$, then ηu satisfies the recurrence

$$u_{n+1} = 6u_n - u_{n-1} + 12\,\eta, \tag{2·2}$$

with, say, $(u_0, u_1) = (4-3\eta, 20-3\eta)$. Equation (2·1) is thus equivalent to finding all perfect powers in the recurrence sequence $\{u_n\}$.

Let $K = \mathbb{Q}(\sqrt{2})$ and write $\epsilon = 1 + \sqrt{2}$ for a fundamental unit of norm -1 in K. Our main observation that permits application of the so-called modular method is the following.

LEMMA 2·1. *If (x, y, p) is a solution to* (2·1) *then there exist integers k, ℓ and s, and an $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that*

$$s\,\epsilon^k\sqrt{2} - \epsilon^\ell \alpha^p = 1, \tag{2·3}$$

where k is odd, $s \in \{-1, 1\}$,

$$\mathrm{Norm}(\alpha) = (-1)^{\ell+1}x \quad \textit{and} \quad -\frac{p-1}{2} \leqslant \ell \leqslant \frac{p-1}{2}. \tag{2·4}$$

Proof. We can rewrite (2·1) as

$$(x^p + 3)^2 - 8 = 8y^2,$$

whereby $4 \mid x^p + 3$ and

$$y^2 - 2\left(\frac{x^p+3}{4}\right)^2 = -1.$$

Hence

$$y + \left(\frac{x^p+3}{4}\right)\sqrt{2} = s\epsilon^k, \tag{2·5}$$

where k is odd.

On the other hand, we can also transform equation (2·1) into

$$\left(\frac{x^p+1}{2}\right)^2 - 2y^2 = -x^p$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

and hence have

$$\left(\frac{x^p+1}{2}\right)+y\sqrt{2}=\epsilon^{\ell}\alpha^p, \tag{2·6}$$

where α and ℓ satisfy (2·4). From (2·5) and (2·6), we deduce (2·3).

3. *Linear forms in logarithms*

The purpose of this section is to prove the following proposition, via an appeal to the theory of linear forms in logarithms.

PROPOSITION 3·1. *If the Diophantine equation*

$$x^{2n}\pm 6x^n+1=8y^2$$

has a solution in positive integers x, n and y, with $x, n>1$, then n is divisible by an odd prime $p<2\cdot 10^{10}$.

Either equation (2·3) or (2·5) is a suitable starting point for deriving a linear form in logarithms leading to an absolute upper bound upon p; we will appeal to the latter. Specifically, from (2·5), we have

$$\frac{|x^p+3|}{4}=\frac{\epsilon^k+\epsilon^{-k}}{2\sqrt{2}}.$$

It follows that

$$\frac{|x|^p}{\sqrt{2}\,\epsilon^{|k|}}-1$$

is "small", whereby the same is true of the linear form

$$\Lambda=p\log|x|-\log\sqrt{2}-|k|\log\epsilon. \tag{3·1}$$

More precisely, it is easy to verify that

$$\log|\Lambda|<-p\log|x|+2. \tag{3·2}$$

For any algebraic number α of degree d over $\mathbb{Q}$, we define as usual the *absolute logarithmic height* of α by the formula

$$h(\alpha)=\frac{1}{d}\left(\log|a_0|+\sum_{i=1}^{d}\log\max\left(1,|\alpha^{(i)}|\right)\right),$$

where a_0 is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and the $\alpha^{(i)}$ are the conjugates of α in the field of complex numbers. The following is the main result of Matveev [**12**, theorem 2·1].

THEOREM 3 (Matveev). *Let $\mathbb{K}$ be an algebraic number field of degree D over $\mathbb{Q}$ and put $\chi=1$ if $\mathbb{K}$ is real, $\chi=2$ otherwise. Suppose that $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{K}^*$ with absolute logarithmic heights $h(\alpha_i)$ for $1\leqslant i\leqslant n$, and suppose that*

$$A_i\geqslant\max\{D\,h(\alpha_i),|\log\alpha_i|\},\ 1\leqslant i\leqslant n,$$

for some fixed choice of the logarithm. Define

$$\Lambda=b_1\log\alpha_1+\cdots+b_n\log\alpha_n,$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

where the b_i are integers and set

$$B = \max\{1, \max\{|b_i| A_i/A_n \ : \ 1 \leqslant i \leqslant n\}\}.$$

Define, with $e := \exp(1)$, further,

$$\Omega = A_1 \cdots A_n,$$

$$C(n) = C(n, \chi) = \frac{16}{n!\chi} e^n (2n + 1 + 2\chi)(n + 2)(4n + 4)^{n+1} (en/2)^{\chi},$$

$$C_0 = \log\left(e^{4.4n+7} n^{5.5} D^2 \log(eD)\right) \ \text{ and } \ W_0 = \log(1.5eBD \log(eD)).$$

Then, if $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over $\mathbb{Z}$ and $b_n \neq 0$, we have

$$\log|\Lambda| > -C(n)\, C_0\, W_0\, D^2\, \Omega.$$

We apply this theorem to our situation, with

$$D = 2, \ \chi = 1, \ n = 3, \ b_3 = p, \ \alpha_3 = |x|,$$

under the assumption that $|x| > 1$. We conclude, after a little work, that

$$\log|\Lambda| > -(88626836156 \log p + 232663287513) \log|x|.$$

Combining this with (3·2) (and using that $|x| \geqslant 7$, an almost immediate consequence of (2·1) and the supposition that $|x| > 1$; succinctly, 2 is a quadratic residue modulo x, whence $x \equiv \pm 1 \pmod 8$), we obtain the upper bound

$$p < 2.772 \cdot 10^{12} =: P_0. \tag{3·3}$$

This bound is the starting point of our analysis. Arguing à la Baker, we may thus find an effective absolute upper bound upon $|x|$ in (the finite collection of hyperelliptic) equations (2·1). Let us assume, for the remainder of this section, that

$$2 \cdot 10^{10} < p < P_0. \tag{3·4}$$

We will show that (2·1) has no solutions for p satisfying (3·4), via appeal to a complicated but slightly sharper lower bound for linear forms in three complex logarithms, due to the third author [**13**, proposition 5·1]).

THEOREM 4 (Mignotte). *Consider three non-zero algebraic numbers α_1, α_2 and α_3, which are either all real and > 1, or all complex of modulus one and all $\neq 1$. Further, assume that the three numbers α_1, α_2 and α_3 are either all multiplicatively independent, or that two of the number are multiplicatively independent and the third is a root of unity. We also consider three positive rational integers b_1, b_2, b_3 with $\gcd(b_1, b_2, b_3) = 1$, and the linear form*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3,$$

where the logarithms of the α_i are arbitrary determinations of the logarithm, but which are all real or all purely imaginary. Suppose further that

$$b_2 |\log \alpha_2| = b_1 |\log \alpha_1| + b_3 |\log \alpha_3| \pm |\Lambda|$$

and put

$$d_1 = \gcd(b_1, b_2) \ \text{ and } \ d_3 = \gcd(b_3, b_2).$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Let $\rho \geqslant e := \exp(1)$ be a real number and set $\lambda = \log \rho$. Let a_1, a_2 and a_3 be real numbers such that

$$a_i \geqslant \rho |\log \alpha_i| - \log |\alpha_i| + 2D\, \mathrm{h}(\alpha_i), \qquad i \in \{1, 2, 3\},$$

where $D = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}] \,/\, [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}]$, and assume further that

$$\Omega := a_1 a_2 a_3 \geqslant 2.5 \ \text{ and } \ a := \min\{a_1, a_2, a_3\} \geqslant 0.62.$$

Let m and L be positive integers with $m \geqslant 3$, $L \geqslant D + 4$ and set $K = [m\Omega L]$. Let χ be fixed with $0 < \chi \leqslant 2$ and define

$$c_1 = \max\{(\chi m L)^{2/3}, \sqrt{2mL/a}\}, \ c_2 = \max\{2^{1/3}\,(mL)^{2/3}, L\sqrt{m/a}\}, \ c_3 = (6m^2)^{1/3} L,$$

$$R_i = [c_i a_2 a_3], \ S_i = [c_i a_1 a_3] \ \text{ and } T_i = [c_i a_1 a_2],$$

for $i \in \{1, 2, 3\}$, and set

$$R = R_1 + R_2 + R_3 + 1, \ S = S_1 + S_2 + S_3 + 1 \ \text{ and } \ T = T_1 + T_2 + T_3 + 1.$$

Define

$$c = \max\left\{\frac{R}{La_2a_3}, \frac{S}{La_1a_3}, \frac{T}{La_1a_2}\right\}.$$

Finally, assume that the quantity

$$\left(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L}\right)\lambda - (D+1)\log L - 3gL^2 c\,\Omega$$

$$-D(K-1)\log B - 2\log K + 2D\log 1.36$$

is positive, where

$$g = \frac{1}{4} - \frac{K^2 L}{12RST} \ \text{ and } \ B = \frac{e^3 c^2 \Omega^2 L^2}{4K^2 d_1 d_3}\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right)\left(\frac{b_3}{a_2} + \frac{b_2}{a_3}\right).$$

Then either

$$\log \Lambda > -(KL + \log(3KL))\lambda, \tag{3·5}$$

or the following condition holds:

either *there exist non-zero rational integers r_0 and s_0 such that*

$$r_0 b_2 = s_0 b_1 \tag{3·6}$$

with

$$|r_0| \leqslant \frac{(R_1+1)(T_1+1)}{M - T_1} \ \text{ and } \ |s_0| \leqslant \frac{(S_1+1)(T_1+1)}{M - T_1}, \tag{3·7}$$

where

$$M = \max\left\{R_1 + S_1 + 1, S_1 + T_1 + 1, R_1 + T_1 + 1, \chi\tau_1^{1/2}\right\}, \ \tau_1 = (R_1+1)(S_1+1)(T_1+1),$$

or *there exist rational integers r_1, s_1, t_1 and t_2, with $r_1 s_1 \neq 0$, such that*

$$(t_1 b_1 + r_1 b_3) s_1 = r_1 b_2 t_2, \qquad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1, \tag{3·8}$$

which also satisfy

$$|r_1 s_1| \leqslant \gcd(r_1, s_1) \cdot \frac{(R_1+1)(S_1+1)}{M - \max\{R_1, S_1\}},$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

$$|s_1 t_1| \leqslant \gcd(r_1, s_1) \cdot \frac{(S_1+1)(T_1+1)}{M - \max\{S_1, T_1\}}$$

and

$$|r_1 t_2| \leqslant \gcd(r_1, s_1) \cdot \frac{(R_1+1)(T_1+1)}{M - \max\{R_1, T_1\}}.$$

Moreover, when $t_1 = 0$ *we can take* $r_1 = 1$*, and when* $t_2 = 0$ *we can take* $s_1 = 1$.

We apply this result with

$$b_2 = p,\ \alpha_2 = |x|,\ b_1 = 1,\ \alpha_1 = \sqrt{2},\ b_3 = |k| \text{ and } \alpha_3 = 1 + \sqrt{2},$$

so that we may take

$$D = 2,\ d_1 = 1,\ d_3 \in \{1, p\},\ a_1 = \frac{\rho+3}{2}\log 2,\ a_2 = (\rho+3)\log|x|$$

and $a_3 = (\rho+1)\log(1+\sqrt{2})$, whence $a = a_1$. Our goal is to choose L, m, ρ and χ such that (3·5) contradicts (3·2), and (3·7) contradicts (3·4), whereby we necessarily have (3·8).

Setting

$$L = 545,\ m = 25,\ \rho = 5 \text{ and } \chi = 2,$$

we find, after a short Maple computation, that, for $3 \cdot 10^{10} < p \leqslant P_0$ and all $|x| \geqslant 7$, we are in situation (3·8), whereby there exist integers r_1, s_1, t_1 and t_2 for which

$$(t_1 + r_1|k|)s_1 = r_1 t_2 p, \tag{3·9}$$

where

$$\left|\frac{r_1 s_1}{\gcd(r_1, s_1)}\right| \leqslant 80 \text{ and } \left|\frac{s_1 t_1}{\gcd(r_1, s_1)}\right| \leqslant 41.$$

Similarly, for $2 \cdot 10^{10} < p < 3 \cdot 10^{10}$, we choose

$$L = 545,\ m = 21,\ \rho = 5 \text{ and } \chi = 2,$$

to deduce the existence of integers r_1, s_1, t_1 and t_2 with (3·9) and

$$\left|\frac{r_1 s_1}{\gcd(r_1, s_1)}\right| \leqslant 75 \text{ and } \left|\frac{s_1 t_1}{\gcd(r_1, s_1)}\right| \leqslant 39.$$

Since, in all cases, we assume that $p > 2 \cdot 10^{10}$, we thus have

$$\max\{|r_1|, |s_1|, |t_1|\} < p.$$

Hence, from the fact that $\gcd(r_1, t_1) = \gcd(s_1, t_2) = 1$, it follows that $r_1 = \pm s_1$, whereby $t_1 + r_1|k| = \pm t_2 p$. Without loss of generality, we may thus write

$$u + r|k| = tp,$$

where $r = |r_1|$ and $t = |t_2|$ are positive integers, $u = \pm t_1$,

$$|u| \leqslant \begin{cases} 41 & \text{if } 3 \cdot 10^{10} < p \leqslant P_0, \\ 39 & \text{if } 2 \cdot 10^{10} < p < 3 \cdot 10^{10} \end{cases}$$

and

$$r \leqslant \begin{cases} 80 & \text{if } 3 \cdot 10^{10} < p \leqslant P_0, \\ 75 & \text{if } 2 \cdot 10^{10} < p < 3 \cdot 10^{10} \end{cases}.$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

The linear form Λ defined in (3·1) may thus be rewritten as a linear form in two logarithms

$$\Lambda = p \log\left(\frac{|x|}{(1+\sqrt{2})^{t/r}}\right) - \log\left(\frac{\sqrt{2}}{(1+\sqrt{2})^{u/r}}\right).$$

We are in position to apply the following state-of-the-art lower bound for linear forms in the logarithms of two algebraic numbers, due to Laurent [**11**, theorem 2]).

THEOREM 5 (Laurent). *Let α_1 and α_2 be multiplicatively independent algebraic numbers, h, ρ and μ be real numbers with $\rho > 1$ and $1/3 \leqslant \mu \leqslant 1$. Set*

$$\sigma = \frac{1+2\mu-\mu^2}{2},\ \lambda = \sigma \log \rho,\ H = \frac{h}{\lambda} + \frac{1}{\sigma},$$
$$\omega = 2\left(1+\sqrt{1+\frac{1}{4H^2}}\right),\ \theta = \sqrt{1+\frac{1}{4H^2}} + \frac{1}{2H}.$$

Consider the linear form $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$, where b_1 and b_2 are positive integers. Put

$$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \,/\, [\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]$$

and assume that

$$h \geqslant \max\left\{D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\lambda + 1.75\right) + 0.06, \lambda, \frac{D\log 2}{2}\right\},$$

$$a_i \geqslant \max\{1, \rho|\log\alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\} \qquad (i = 1, 2),$$

and

$$a_1 a_2 \geqslant \lambda^2.$$

Then

$$\log|\Lambda| \geqslant -C\left(h + \frac{\lambda}{\sigma}\right)^2 a_1 a_2 - \sqrt{\omega\theta}\left(h + \frac{\lambda}{\sigma}\right) - \log\left(C'\left(h + \frac{\lambda}{\sigma}\right)^2 a_1 a_2\right) \qquad (3{\cdot}10)$$

with

$$C = \frac{\mu}{\lambda^3\sigma}\left(\frac{\omega}{6} + \frac{1}{2}\sqrt{\frac{\omega^2}{9} + \frac{8\lambda\omega^{5/4}\theta^{1/4}}{3\sqrt{a_1 a_2}H^{1/2}} + \frac{4}{3}\left(\frac{1}{a_1} + \frac{1}{a_2}\right)\frac{\lambda\omega}{H}}\right)^2$$

and

$$C' = \sqrt{\frac{C\sigma\omega\theta}{\lambda^3\mu}}.$$

We apply this result with

$$b_1 = 1,\ b_2 = p,\ \alpha_1 = \frac{\sqrt{2}}{(1+\sqrt{2})^{u/r}} \text{ and } \alpha_2 = \frac{|x|}{(1+\sqrt{2})^{t/r}},$$

so that $D = 2r$,

$$h(\alpha_1) \leqslant \frac{\log 2}{2} + \frac{|u|}{2r}\log(1+\sqrt{2}) \text{ and } h(\alpha_2) \leqslant \log|x| + \frac{t}{2r}\log(1+\sqrt{2}).$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Further, we may choose

$$a_1 = \left(2r + \frac{\rho - 1}{2}\right)\log 2 + |u|\left(2 + \frac{\rho + 1}{r}\right)\log(1 + \sqrt{2})$$

and

$$a_2 = (8r + 1)\log|x|.$$

That this latter choice is a valid one follows from the fact that $|x|^p > (1 + \sqrt{2})^{|k|}$, whereby

$$t < \left(\frac{u}{|k|} + r\right)\frac{\log|x|}{\log(1 + \sqrt{2})},$$

and the assumption that $\rho < 10^6$, say.

Choosing $\rho = 283$ and $\mu = 0.6$, we find, for $p > 3 \cdot 10^{10}$, $|x| \geqslant 7$ and all $-41 \leqslant u \leqslant 41$, $1 \leqslant r \leqslant 80$, that inequality (3·10) contradicts (3·2), whilst the same is true (with identical parameter choices), for primes p with $2 \cdot 10^{10} < p < 3 \cdot 10^{10}$, $-38 \leqslant u \leqslant 38$, $1 \leqslant r \leqslant 75$. The final case is when $(r, u) = (75, \pm 39)$ which reduces immediately to that with $(r_0, u_0) = (25, \pm 13)$ upon dividing by the $\gcd(r, u)$.

Proposition 3·1 thus follows, as desired.

4. *Frey curves and Hilbert modular forms*

4·1. *The Frey curve*

We next return to solutions to (2·1), to which we shall now associate a Frey curve:

$$E_{s,k} \;:\; Y^2 = X(X + 1)(X + s \cdot \epsilon^k\sqrt{2}) \tag{4·1}$$

where the choice of sign $s = \pm 1$ and the value of k arises from Lemma 2·1. By an easy application of Tate's algorithm we find the following.

LEMMA 4·1. *The curve $E_{s,k}$ has minimal discriminant*

$$\Delta_{\min} = 32\epsilon^{2(k+\ell)}\alpha^{2p}$$

and conductor

$$\mathfrak{N} = (\sqrt{2})^9 \cdot \prod_{\mathfrak{q}|\alpha} \mathfrak{q}.$$

Our goal is to use the arithmetic of this Frey curve to show that any solution to (2·1) necessarily closely resembles one of the "trivial" ones with $x = 1$ and $y = k = \pm 1$.

4·2. *Irreducibility*

We shall make use of the following result due to Freitas and Siksek [**9**], which is based on the work of David [**6**] and Momose [**14**].

PROPOSITION 4·2. *Let K be a totally real Galois number field of degree d, with ring of integers $\mathcal{O}_K$ and Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $S = \{0, 12\}^G$, which we think of as the set of sequences of values 0, 12 indexed by $\tau \in G$. For $\mathbf{s} = (s_\tau) \in S$ and $\alpha \in K$, define the* ***twisted norm associated to*** $\mathbf{s}$ *by*

$$\mathcal{N}_{\mathbf{s}}(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}.$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Let $\epsilon_1, \ldots, \epsilon_{d-1}$ be a basis for the unit group of K, and define

$$A_{\mathbf{s}} := \mathrm{Norm}\left(\gcd((\mathcal{N}_{\mathbf{s}}(\epsilon_1) - 1)\mathcal{O}_K, \ldots, (\mathcal{N}_{\mathbf{s}}(\epsilon_{d-1}) - 1)\mathcal{O}_K)\right). \tag{4·2}$$

Let B be the least common multiple of the $A_{\mathbf{s}}$ taken over all $\mathbf{s} \neq (0)_{\tau\in G}, (12)_{\tau\in G}$. Let $p \not| B$ be a rational prime, unramified in K, such that $p \geqslant 17$ or $p = 11$. Let E/K be an elliptic curve, and $\mathfrak{q} \not| p$ be a prime of good reduction for E. Define

$$P_{\mathfrak{q}}(X) = X^2 - a_{\mathfrak{q}}(E)X + \mathrm{Norm}(\mathfrak{q})$$

to be the characteristic polynomial of Frobenius for E at $\mathfrak{q}$. Let $r \geqslant 1$ be an integer such that $\mathfrak{q}^r$ is principal. If E is semistable at all $\mathfrak{p} \mid p$ and $\overline{\rho}_{E,p}$ is reducible then

$$p \mid \mathrm{Res}(P_{\mathfrak{q}}(X),\ X^{12r} - 1) \tag{4·3}$$

where Res *denotes the resultant of the two polynomials.*

We now return to the case where $E = E_{s,k}$ is our Frey curve (4·1).

LEMMA 4·3. *For $E = E_{s,k}$ as above, $\overline{\rho}_{E,p}$ is irreducible for $p \geqslant 5$.*

Proof. We suppose first that $p \geqslant 17$ or $p = 11$, and apply Proposition 4·2. The constant B in the proposition is simply

$$B = \mathrm{Norm}(\epsilon^{12} - 1) = -2^5 \cdot 5^2 \cdot 7^2,$$

whereby if $p \geqslant 11$ then $p \not| B$. Suppose that $\overline{\rho}_{E,p}$ is reducible. From (2·1), if $q \equiv 3, 5 \pmod 8$ then $q \not| x$ and so E has good reduction at (the inert prime) q.

We write μ_q for the multiplicative order of ϵ modulo q. Note that the trace $a_q(E_{s,k})$ depends only on the choice of sign $s = \pm 1$ and on the value of k modulo μ_q. We shall restrict our attention to the following set of primes

$$Q = \{3, 5, 11, 13, 19, 29, 43, 59, 83, 109, 131, 139, 251, 269, 307, 419, 461, 659\}.$$

The primes $q \in Q$ satisfy $q \equiv 3, 5 \pmod 8$ and also

$$\mu_q \mid 9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11.$$

Recall also that k is odd, and that $\pm\epsilon^k\sqrt{2} - 1 = \epsilon^{\ell}\alpha^p \not\equiv 0 \pmod q$. Let

$$S = \{(t, m)\ :\ 0 \leqslant m < 9240 \text{ odd},\ t = \pm 1,\ q \not| (t \cdot \epsilon^m\sqrt{2} - 1) \text{ for all } q \in Q\}. \tag{4·4}$$

It is clear that there is some $(t, m) \in S$ such that $a_q(E_{s,k}) = a_q(E_{t,m})$ for all $q \in Q$. By Proposition 4·2, we see that p divides $R_{(t,m)}$ where

$$R_{(t,m)} = \gcd\{\mathrm{Res}(x^{12} - 1, x^2 - a_q(E_{t,m})x + q^2)\ :\ q \in Q\}.$$

Using a short `Magma` [**2**] script, we computed $R_{(t,m)}$ for $(t, m) \in S$ and checked that $R_{(t,m)}$ is divisible only by powers of 2, 3, 5, 7 and 13. Thus $\overline{\rho}_{E,p}$ is irreducible for $p \geqslant 17$ or $p = 11$.

We now briefly treat $p \in \{5, 7, 13\}$. In each case, we will in fact show that there is no elliptic curve E/K with full 2-torsion and a p-isogeny. Here we found `Magma`'s built-in `Small Modular Curve` package invaluable.

(a) An elliptic curve E/K with full 2-torsion and a 5-isogeny is isogenous over K to an elliptic curve with a 20-isogeny, and so gives rise to a non-cuspidal K-point on $X_0(20)$. A model for $X_0(20)$ is given by the elliptic curve

$$X_0(20)\ :\ y^2 = x^3 + x^2 + 4x + 4,$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

which has Cremona reference 20A1. This has rank 0 over K, and in fact a full list of K-points is $\{\infty, (4, \pm 10), (0, \pm 2), (-1, 0)\}$. These points are all cuspidal, completing the proof for $p = 5$.

(b) An elliptic curve E/K with a 7-isogeny and a point of order 2 gives rise to a non-cuspidal K-point on $X_0(14)$. A model for $X_0(14)$ is given by the elliptic curve

$$X_0(14) \ : \ y^2 + xy + y = x^3 + 4x - 6,$$

which has Cremona reference 14A1. This again has rank 0 over K. The K-points are $\{\infty, (9, 23), (1, -1), (2, -5), (9, -33), (2, 2)\}$. The first four points are cusps. The last two correspond to elliptic curves with j-invariants -3375 and 16581375. It turns out that elliptic curves with these j-invariants have only one point of order 2 over K. This completes the proof for $p = 7$.

(c) An elliptic curve E/K with a 13-isogeny and a point of order 2 gives rise to a non-cuspidal K-point on $X_0(26)$, which has genus 2. We shall in fact work with $X_0(26)/\langle w_{13} \rangle$, where w_{13} is the Atkin-Lehner involution. This quotient is the elliptic curve with Cremona reference 26B1:

$$X_0(26)/\langle w_{13} \rangle \ : \ y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Again this has rank 0 over K, and a full list of K-points is given by

$$\{\infty, (-1, -2), (-1, 2), (1, -2), (1, 0), (3, -6), (3, 2)\}.$$

The only K-points we obtain by pulling back to $X_0(26)$ are cusps. This completes the proof.

4·3. *Level-lowering*

Suppose that $p \geqslant 5$. By [**7**], elliptic curves over real quadratic fields are modular; in particular E is modular. We now apply the standard level-lowering recipe found in [**8**] and based on theorems of Fujiwara, Jarvis and Rajaei (it is here that we require Lemma 4·3). From the recipe we know that $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,\mathfrak{p}}$ for some Hilbert newform over K of level $\mathfrak{M} = (\sqrt{2})^9$ and prime ideal $\mathfrak{p} \mid p$. Using `Magma`, we find that the space of Hilbert newforms of level $\mathfrak{M}$ is 8-dimensional, and in fact decomposes into 8 rational eigenforms.

Through a small search, we found 8 elliptic curves over K of conductor $\mathfrak{M}$. By computing their traces at small prime ideals, we checked that they are in fact pairwise non-isogenous. These elliptic curves are all modular by the same theorem cited above, and hence must correspond to the 8 Hilbert newforms of level $\mathfrak{M}$. Thus $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_i,p}$ where $F_1, \ldots, F_8$ are the 8 elliptic curves given as follows:

$$F_1 \ : \ Y^2 = X^3 + \sqrt{2}X^2 + (\sqrt{2} - 1)X,$$
$$F_2 \ : \ Y^2 = X^3 + (-\sqrt{2} + 3)X^2 + (-\sqrt{2} + 2)X,$$
$$F_3 \ : \ Y^2 = X^3 + (2\sqrt{2} - 1)X^2 + (-\sqrt{2} + 2)X,$$
$$F_4 \ : \ Y^2 = X^3 + (\sqrt{2} - 2)X^2 + (-\sqrt{2} + 1)X,$$
$$F_5 \ : \ Y^2 = X^3 + (-\sqrt{2} + 1)X^2 - \sqrt{2}X,$$
$$F_6 \ : \ Y^2 = X^3 + (\sqrt{2} - 1)X^2 - \sqrt{2}X,$$
$$F_7 \ : \ Y^2 = X^3 + (\sqrt{2} + 3)X^2 + (\sqrt{2} + 2)X,$$
$$F_8 \ : \ Y^2 = X^3 - \sqrt{2}X^2 + (-\sqrt{2} - 1)X.$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

LEMMA 4·4. *Let $E = E_{s,k}$ and let F be one of the eight elliptic curves $F_1, \ldots, F_8$ above. Suppose that $\overline{\rho}_{E,p} \sim \overline{\rho}_{F,p}$ and let $\mathfrak{q} \nmid 2$ be a prime ideal of K, and q be the rational prime such that $\mathfrak{q} \mid q$.*

(i) *If* $\mathfrak{q} \nmid (s\epsilon^k\sqrt{2} - 1)$ *then* $a_{\mathfrak{q}}(E) \equiv a_{\mathfrak{q}}(F) \pmod{p}$.
(ii) *If* $\mathfrak{q} \mid (s\epsilon^k\sqrt{2} - 1)$ *and* $q \not\equiv 7 \pmod 8$ *then* $\mathrm{Norm}(\mathfrak{q}) + 1 \equiv a_{\mathfrak{q}}(F) \pmod{p}$.
(iii) *If* $\mathfrak{q} \mid (s\epsilon^k\sqrt{2} - 1)$ *and* $q \equiv 7 \pmod 8$ *then* $\mathrm{Norm}(\mathfrak{q}) + 1 \equiv -a_{\mathfrak{q}}(F) \pmod{p}$.

Proof. From the model (4·1), it is easy to see that $E_{s,k}$ has good reduction at $\mathfrak{q}$ in case (i), split multiplicative reduction in case (ii) and non-split multiplicative reduction in case (iii). If $q \neq p$, the lemma follows by comparing traces of the images of Frobenius at $\mathfrak{q}$ for the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{F,p}$. For $q = p$ see [**10**, proposition 3].

LEMMA 4·5. *The $s = \pm 1$ sign in (2·3), (2·5) and (4·1) is in fact $+1$. Moreover, either $k \equiv -1 \pmod{9240}$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_2,p}$ or $k \equiv 1 \pmod{9240}$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_7,p}$.*

Proof. We shall use ideas from the proof of Lemma 4·3. For a prime ideal $\mathfrak{q}$ we let $\mu_{\mathfrak{q}}$ be the order of ϵ modulo $\mathfrak{q}$. In the proof of Lemma 4·3, we restricted ourselves to inert primes. It is useful to now also use split primes. Let

$$\mathfrak{Q} = \{\mathfrak{q} \ : \ \mu_{\mathfrak{q}} \mid 9240, \quad 3 \leqslant \mathrm{Norm}(\mathfrak{q}) < 1000\}.$$

Fix $i \in \{1, 2, \ldots, 8\}$ and suppose $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_i,p}$ where $E = E_{s,k}$. We let S be given by (4·4), whereby we know that there is some $(t, m) \in S$ such that $s = t$ and $k \equiv m \pmod{9240}$. Let $\mathfrak{q} \in \mathfrak{Q}$, and let q be the rational prime satisfying $\mathfrak{q} \mid q$. By Lemma 4·4 we have the following:

(a) if $\mathfrak{q} \nmid (t\epsilon^m\sqrt{2} - 1)$ then $a_{\mathfrak{q}}(E_{t,m}) = a_{\mathfrak{q}}(E_{s,k}) \equiv a_{\mathfrak{q}}(F_i) \pmod{p}$;
(b) if $\mathfrak{q} \mid (t\epsilon^m\sqrt{2} - 1)$ and $q \not\equiv 7 \pmod 8$ then $\mathrm{Norm}(\mathfrak{q}) + 1 \equiv a_{\mathfrak{q}}(F_i) \pmod{p}$;
(c) if $\mathfrak{q} \mid (t\epsilon^m\sqrt{2} - 1)$ and $q \equiv 7 \pmod 8$ then $\mathrm{Norm}(\mathfrak{q}) + 1 \equiv -a_{\mathfrak{q}}(F_i) \pmod{p}$.

Define

$$\beta_{t,m,i}(\mathfrak{q}) = \begin{cases} a_{\mathfrak{q}}(E_{t,m}) - a_{\mathfrak{q}}(F_i) & \text{if } \mathfrak{q} \nmid (t\epsilon^m\sqrt{2} - 1) \\ \mathrm{Norm}(\mathfrak{q}) + 1 - a_{\mathfrak{q}}(F_i) & \text{if } \mathfrak{q} \mid (t\epsilon^m\sqrt{2} - 1) \text{ and } q \not\equiv 7 \pmod 8 \\ \mathrm{Norm}(\mathfrak{q}) + 1 + a_{\mathfrak{q}}(F_i) & \text{if } \mathfrak{q} \mid (t\epsilon^m\sqrt{2} - 1) \text{ and } q \equiv 7 \pmod 8 . \end{cases}$$

We let

$$\gamma_{t,m,i} = \gcd(\beta_{t,m,i}(\mathfrak{q}) : \mathfrak{q} \in \mathfrak{Q}).$$

Note that if $s = t$, $k \equiv m \pmod{9240}$ and $\rho_{E,p} \sim \rho_{F_i,p}$, then $p \mid \gamma_{t,m,i}$. Using a `Magma` script, we computed $\gamma_{t,m,i}$ for all $(t, m) \in S$ and $i \in \{1, 2, \ldots, 8\}$. We found that all of these are divisible only by 2 and 3, except for $\gamma_{1,9239,2}$ and $\gamma_{1,1,7}$ which are both zero. Hence $s = +1$, and either $k \equiv -1 \pmod{9240}$ and $F_i = F_2$ or $k \equiv 1 \pmod{9240}$ and $F_i = F_7$.

Note, in fact, that F_2 is isomorphic to $E_{1,-1}$ and F_7 is isomorphic to $E_{1,1}$ (which explains why $\gamma_{1,9239,2} = \gamma_{1,1,7} = 0$).

We now simplify our Frey curve in (4·1) to take account of the sign $s = +1$. We denote the new Frey curve by

$$E_k \ : \ Y^2 = X(X + 1)(X + \epsilon^k\sqrt{2}).$$

Equations (2·1) and (2·3) satisfy the following useful symmetry.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

LEMMA 4·6. *Let* (x, y, k, ℓ, α) *be a solution to equations* (2·1) *and* (2·3)*, satisfying* (2·4)*. Then* $(x, -y, -k, -\ell, (-1)^{\ell}\overline{\alpha})$ *is also a solution to equations* (2·1) *and* (2·3)*, also satisfying* (2·4).

Proof. The lemma follows on conjugating equations (2·3) and (2·5), observing that $\overline{\epsilon} = -\epsilon^{-1}$, and recalling that k is odd.

5. *Arithmetic information from Frey curves*

We continue with the same notation as in the previous section. Our basic goal is to obtain lower bounds for the exponent $|k|$ in the event that $k \neq 1$.

5·1. *Sieving: part* I

We begin by sharpening (part of) Lemma 4·5.

PROPOSITION 5·1. *Suppose that* $p \geqslant 19$ *and let*

$$M = 9240 \prod_{\substack{3 \leqslant \ell < 2.4 \times 10^5 \\ \ell \text{ prime}}} \ell. \tag{5·1}$$

Then $k \equiv \pm 1 \pmod{M}$. *In particular,* $k = \pm 1$ *or* $\log_{10} |k| \geqslant 103944$.

Proof. We start by defining $M_0 = 9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. We know from Lemma 4·5 that $k \equiv \pm 1 \pmod{M_0}$. By Lemma 4·6, we may assume that $k \equiv 1 \pmod{M_0}$, and will use this to deduce that $k \equiv 1 \pmod{M}$. It then plainly follows that if $k \equiv -1 \pmod{M_0}$ then $k \equiv -1 \pmod{M}$.

Suppose $k \equiv 1 \pmod{M_0}$. Let

$$\ell_1 = 3, \quad \ell_2 = 5, \quad \ell_3 = 7, \ldots$$

be the sequence of primes starting with 3. We define $M_n = \ell_n \cdot M_{n-1}$. We will show inductively that $k \equiv 1 \pmod{M_n}$ until $M_n = M$. A direct computation, showing that M somewhat exceeds 10^{103944}, yields the last statement in the proposition.

For the inductive step, suppose $k \equiv 1 \pmod{M_{n-1}}$. Our strategy is to write down a small set $\mathfrak{Q}$ of odd prime ideals $\mathfrak{q}$ of K satisfying

$$\ell_n \mid \mu_{\mathfrak{q}}, \qquad \mu_{\mathfrak{q}} \mid M_n;$$

here as before, $\mu_{\mathfrak{q}}$ is the multiplicative order of ϵ modulo $\mathfrak{q}$. Let

$$\mathcal{K} = \{1, 1 + M_{n-1}, 1 + 2M_{n-1}, \ldots, 1 + (\ell_n - 1)M_{n-1}\}.$$

We know that $k \equiv m \pmod{M_n}$ for some $m \in \mathcal{K}$. By the previous section, p divides $\beta_{1,m,7}(\mathfrak{q})$ for all $\mathfrak{q} \in \mathfrak{Q}$. For $m \in \mathcal{K}$, we compute $\gcd_{\mathfrak{q} \in \mathfrak{Q}}(\beta_{1,m,7}(\mathfrak{q}))$. With a sufficiently large enough initial set $\mathfrak{Q}$, we found that this gcd is divisible only by primes $\leqslant 17$ unless $m = 1$ (in which case it is 0). This shows that $k \equiv 1 \pmod{M_n}$. The `Magma` script executing this proof took roughly 218 hours to run on a 2200MHz AMD Opteron.

5·2. *Sieving: part* II

In view of Proposition 5·1, we suppose $k \equiv \pm 1 \pmod{M}$ where M is given by (5·1). The objective of this subsection is to show the following.

PROPOSITION 5·2. *For primes* $19 \leqslant p < 2 \cdot 10^{10}$ *we have* $k \equiv \ell \equiv \pm 1 \pmod{p}$*, where* k *and* ℓ *are the exponents in* (2·3)*. In particular, via* (2·4)*, we have that* $\ell = \pm 1$.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

We shall suppose that $k \equiv 1 \pmod{M}$ and deduce $k \equiv \ell \equiv 1 \pmod{p}$. The Proposition then follows from Lemma 4·6. Fix $p \geqslant 19$. Inspired by [**5**, lemma 7·4], we choose an auxiliary integer q satisfying certain conditions, which we enumerate as needed. The first two conditions are the following:

(i) $q \equiv 1 \pmod{8}$ is prime;
(ii) $q = np + 1$, where n is an integer.

Fix $\delta \in \mathbb{F}_q$ satisfying $\delta^2 \equiv 2 \pmod{q}$ (which we may do, via assumption (i)). Let

$$\mathfrak{q}_1 = q\mathcal{O}_K + (\sqrt{2} - \delta)\mathcal{O}_K \quad \text{and} \quad \mathfrak{q}_2 = q\mathcal{O}_K + (\sqrt{2} + \delta)\mathcal{O}_K.$$

Then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are prime ideals with residue field $\mathbb{F}_q$,

$$\sqrt{2} \equiv \delta \pmod{\mathfrak{q}_1} \quad \text{and} \quad \sqrt{2} \equiv -\delta \pmod{\mathfrak{q}_2}.$$

Let

$$\mathcal{F}_1 \ : \ Y^2 = X^3 + (\delta + 3)X^2 + (\delta + 2)X$$

and

$$\mathcal{F}_2 \ : \ Y^2 = X^3 + (-\delta + 3)X^2 + (-\delta + 2)X.$$

These are the reductions of F_7 modulo $\mathfrak{q}_1$ and $\mathfrak{q}_2$, respectively. We shall suppose that q is chosen so that the following condition on the traces of $\mathcal{F}_i$ is satisfied.

(iii) $a_q(\mathcal{F}_i) \not\equiv \pm 2 \pmod{p}$ for $i = 1, 2$.

Note that $q \equiv 1 \pmod{p}$ by condition (ii). By Lemma 4·4, we see that

$$\mathfrak{q}_i \nmid (\epsilon^k \sqrt{2} - 1).$$

Thus by Lemma 2·1, $q \nmid x$. Appealing to Lemma 4·4 again, we have

$$a_{\mathfrak{q}_1}(E_k) \equiv a_q(\mathcal{F}_1) \pmod{p} \quad \text{and} \quad a_{\mathfrak{q}_2}(E_k) \equiv a_q(\mathcal{F}_2) \pmod{p}. \tag{5·2}$$

By (2·5) and Lemma 4·5, we have

$$y + \left(\frac{x^p + 3}{4}\right)\sqrt{2} = \epsilon^k,$$

whence, using the fact that k is odd,

$$\left(\frac{x^p + 3}{2}\right)\sqrt{2} = \epsilon^k + \epsilon^{-k}. \tag{5·3}$$

Let

$$\mu_n(\mathbb{F}_q) = \{\mu \in \mathbb{F}_q^* \ : \ \mu^n \equiv 1 \pmod{q}\},$$

whereby, as $q \nmid x$ and $q = np + 1$, we see that

$$(x^p \mod q) \in \mu_n(\mathbb{F}_q).$$

Let

$$\mathcal{W}_q = \left\{ e \in \mathbb{F}_q \ : \ e + e^{-1} = \frac{(\mu + 3)\delta}{2} \text{ for some } \mu \in \mu_n(\mathbb{F}_q) \right\}.$$

By (5·3), we have that

$$\epsilon^k \equiv e \pmod{\mathfrak{q}_1} \quad \text{and} \quad \epsilon^k \equiv -e^{-1} \pmod{\mathfrak{q}_2}, \tag{5·4}$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

for some $e \in \mathcal{W}_q$. Moreover, since $\mathfrak{q}_i \not\mid (\epsilon^k\sqrt{2}-1)$, if we define

$$\mathcal{X}_q = \{e \in \mathcal{W}_q \ : \ e \not\equiv \delta^{\pm 1} \pmod{q}\},$$

then necessarily (5·3) holds for some $e \in \mathcal{X}_q$. In practice, we hope to be able to find a prime q satisfying the foregoing and forthcoming conditions, with n small. Computing $\mathcal{W}_q$ amounts to solving n quadratic equations in $\mathbb{F}_q$. The size of $\mathcal{W}_q$ and thus $\mathcal{X}_q$ is at most $2n$. Thus we know that the reduction of ϵ^k modulo $\mathfrak{q}_1$ belongs to this relatively small set. We will now refine $\mathcal{X}_q$, defining subsets $\mathcal{Y}_q$, and $\mathcal{Z}_q$ that also contain the reduction of ϵ^k modulo $\mathfrak{q}_1$. To do this, also suppose that q is chosen so that the following condition is satisfied:

(iv) $n \mid M$.

Since $k \equiv 1 \pmod{M}$, we see that $(q-1) \mid (k-1)p$, whereby

$$(\epsilon^{k-1})^p \equiv 1 \pmod{\mathfrak{q}_i}.$$

Note that $\epsilon \equiv 1+\delta \pmod{\mathfrak{q}_1}$. Let

$$\mathcal{Y}_q = \left\{ e \in \mathcal{X}_q \ : \ \left(\frac{e}{1+\delta}\right)^p \equiv 1 \pmod{q} \right\}.$$

We see that (5·4) holds for some $e \in \mathcal{Y}_q$. Heuristically, the probability that a random element of $\mathcal{X}_q$ belongs to $\mathcal{Y}_q$ is $1/n$. Since $\#\mathcal{X}_q \leqslant 2n$, we expect that $\#\mathcal{Y}_q = O(1)$.

For the next refinement, we will use information derived from the modular approach, as given in (5·2). Write

$$\mathcal{E}_{1,e} \ : \ Y^2 = X(X+1)(X+e\cdot\delta) \ \text{ and } \ \mathcal{E}_{2,e} \ : \ Y^2 = X(X+1)(X+e^{-1}\cdot\delta).$$

Given (5·4), these two elliptic curves over $\mathbb{F}_q$ are the reductions of the Frey curve E_k modulo $\mathfrak{q}_1$, $\mathfrak{q}_2$. Let $\mathcal{Z}_q$ be the set of $e \in \mathcal{Y}_q$ such that

$$a_q(\mathcal{E}_{1,e}) \equiv a_q(\mathcal{F}_1) \pmod{p} \ \text{ and } \ a_q(\mathcal{E}_{2,e}) \equiv a_q(\mathcal{F}_2) \pmod{p}.$$

We know from (5·2) that (5·4) holds for some $e \in \mathcal{Z}_q$. Note that $\mathcal{Z}_q$ cannot be empty, as the value $k=1$ leads to a solution to our original equation (2·1). Thus certainly, $1+\delta$ (which is the reduction of ϵ modulo $\mathfrak{q}_1$) must appear in $\mathcal{Z}_q$. This, of course, is a useful check on the correctness of our computations.

It is reasonable to expect on probabilistic grounds that $\mathcal{Z}_q = \{1+\delta\}$. In fact, this is one of our two final assumptions on q:

(v) $\mathcal{Z}_q = \{1+\delta\}$;
(vi) $(1+\delta)^n \not\equiv 1 \pmod{q}$.

From (v), we see that

$$(1+\delta)^k \equiv \epsilon^k \equiv 1+\delta \pmod{\mathfrak{q}_1}.$$

Thus the multiplicative order of $1+\delta$ in $\mathbb{F}_q^*$ divides $k-1$. Since $q-1=np$, we have from (vi) that this multiplicative order must be divisible by p. Therefore, $k \equiv 1 \pmod{p}$. We now turn our attention to ℓ. Reducing (2·3) modulo $\mathfrak{q}_1$ (and recalling the value of the sign from Lemma 4·5) we have

$$(1+\delta)\delta - (1+\delta)^\ell \alpha^p \equiv 1 \pmod{\mathfrak{q}_1}.$$

As $\delta^2 \equiv 2 \pmod{\mathfrak{q}_1}$, it follows that

$$(1+\delta)^\ell \alpha^p \equiv 1+\delta \pmod{\mathfrak{q}_1}$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

and so

$$(1+\delta)^{n(\ell-1)} \equiv \alpha^{-np} \equiv 1 \pmod{\mathfrak{q}_1}.$$

From (vi), we conclude that $\ell \equiv 1 \pmod{p}$. The following lemma summarizes the above.

LEMMA 5·3. *Suppose $k \equiv 1 \pmod{M}$. Suppose there is a prime q satisfying conditions* (i)–(vi). *Then*

$$k \equiv \ell \equiv 1 \pmod{p}.$$

Proof of Proposition 5·2. As observed previously, it is sufficient to suppose that $k \equiv 1 \pmod{M}$ and show that $k \equiv \ell \equiv 1 \pmod{p}$, for primes p in the range $19 \leqslant p < 2 \cdot 10^{10}$. We used a `Magma` script which for each prime p in this range, finds a prime q satisfying conditions (i)–(vi) above. The total processor time for the proof is roughly 1946 hours, although the computation, running on a 2200MHz AMD Opteron, was spread over 10 processors, making the actual computation time less than nine days.

6. *Reducing our upper bound on p*

From Proposition 3·1, we may suppose that $p < 2 \cdot 10^{10}$. The goal of this section is to reduce this upper bound still further. Let $p \geqslant 19$. We have, according to Lemma 4·5, that $s = 1$ in (2·3). We will assume for the remainder of this section that $k > 1$. Appealing to Proposition 5·2, there exists a positive integer k_0 such that $k = pk_0 \pm 1$, whereby we may now rewrite

$$\epsilon^k \sqrt{2} - \epsilon^l \alpha^p = 1$$

as one of

$$\alpha^p - \sqrt{2}\left(\epsilon^{k_0}\right)^p = \pm 1 - \sqrt{2}, \tag{6·1}$$

so that

$$0 < \Lambda_1 = \log(\sqrt{2}) - p \log\left(\frac{\alpha}{\epsilon^{k_0}}\right) < \epsilon \cdot \alpha^{-p}. \tag{6·2}$$

Applying Theorem 5, with

$$b_2 = 1,\ \alpha_2 = \sqrt{2},\ b_1 = p,\ \alpha_1 = \alpha/\epsilon^{k_0} \text{ and } D = 2,$$

we may take

$$a_1 = (\rho - 1)\frac{\log 2}{2p} + 2\log(\alpha) + 4h(\alpha) \leqslant (\rho - 1)\frac{\log 2}{2p} + 6\log(\alpha)$$

and

$$a_2 = \left(\frac{\rho + 3}{2}\right)\log 2.$$

We choose $\rho = 27$ and $\mu = 1/3$, whereby a short calculation ensures that inequality (3·10), together with the fact that $\alpha \geqslant \sqrt{7}$, contradicts (6·2) for $p > 1637$. Computing the first 10^7 terms in recursion (2·2), verifying that none of them coincide with solutions to (2·1) and noting that the 10^7th term exceeds $\exp(8.8 \cdot 10^6)$, we thus have $|x| > 10^{2348}$ and hence $|\alpha| > 10^{1174}$. Now choosing $\rho = 31$ and $\mu = 1/3$ in Theorem 5, and using our new lower bound upon α, we find that $p \leqslant 941$.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

6·1. *Handling the values of* $19 \leqslant p \leqslant 941$

From equation (6·1), it suffices to solve the family of Thue equations

$$X^p - \sqrt{2}\, Y^p = \pm 1 - \sqrt{2}, \tag{6·3}$$

in integers $X, Y \in \mathbb{Z}[\sqrt{2}]$, for primes p with $19 \leqslant p \leqslant 941$, to handle (2·1) for these values of p. We will do this under the additional assumption that

$$Y = \epsilon^{k_0} > 1.$$

We argue as in the proof of [**5**, proposition 9·3]. Define $\omega = 2^{1/2p}$ to be real and positive and let ζ be a primitive p-th root of unity. Set $K = \mathbb{Q}(\omega)$ and $L = \mathbb{Q}(\omega, \zeta)$. It is straightforward to check that an integral basis for K is $1, \omega, \ldots, \omega^{2p-1}$, and to use this to deduce that the discriminant of K is $D_K = 2^{4p-1} p^{2p}$. Moreover, the unit rank of K is p and its Galois closure is L. We write $\epsilon_{1,1}, \ldots, \epsilon_{1,p}$ for a system of fundamental units of K which, via [**5**, lemma 9·6], we may suppose to satisfy

$$\prod_{i=1}^{p} h(\epsilon_{1,i}) \leqslant 2^{1-p} (p!)^2 (2p)^{-p} R_K, \tag{6·4}$$

where R_K denotes the regulator of K. Further, the absolute values of the inverse of the regulator matrix corresponding to $\epsilon_{1,1}, \ldots, \epsilon_{1,p}$ are bounded above by $(p!)^2 2^{-p} \log^3(6p)$. There thus exist integers $b_1, \ldots, b_p$ such that

$$X - \omega Y = \pm \epsilon_{1,1}^{b_1} \cdots \epsilon_{1,p}^{b_p},$$

where

$$B = \max\{|b_1|, \ldots, |b_p|\} \leqslant 2^{1-p} p (p!)^2 \log^3(6p)\, h(X - \omega Y).$$

We will assume that k is positive; the argument for negative k is similar and leads to an identical conclusion. From (6·3), considering imaginary parts, we have that

$$|X - \omega Y| = (\sqrt{2} \pm 1) \prod_{i=1}^{p-1} \left|X - \omega \zeta^i Y\right|^{-1} \leqslant (\sqrt{2} + 1)\, \omega^{1-p}\, |Y|^{1-p} \prod_{i=1}^{(p-1)/2} \sin^{-2}(\pi i / p),$$

whence

$$|X - \omega Y| < 2^p\, |Y|^{1-p}. \tag{6·5}$$

It follows that

$$\left|X - \omega \zeta^j Y\right| \leqslant \omega |Y| \left|1 - \zeta^j\right| + 2^p\, |Y|^{1-p} < 2.1\, |Y|,$$

where, from the assumption that $k > 1$, we have

$$\log |Y| = \frac{k \pm 1}{p} \log(1 + \sqrt{2}) \geqslant \frac{M}{p} \log(1 + \sqrt{2}) > 10^{103942} \log(1 + \sqrt{2}). \tag{6·6}$$

Here, M is as in Proposition 5·1. We therefore estimate that

$$h(X - \omega Y) < 0.75 + \log |Y| < 1.01 \log |Y|,$$

whereby, crudely,

$$B < p^{2p} \log |Y|. \tag{6·7}$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Define $\epsilon_{2,i}$ and $\epsilon_{3,i}$ for $1 \leqslant i \leqslant p$ as the images under σ and σ^2 of $\epsilon_{1,i}$, where σ is the field automorphism that sends ω to $\omega\zeta$ and fixes ζ. If, following Siegel, we set

$$\lambda = \frac{-\zeta}{1+\zeta} \cdot \frac{X - \omega Y}{X - \zeta\omega Y} = \frac{X - \zeta^2\omega Y}{X - \zeta\omega Y} \cdot \frac{1}{1+\zeta} - 1,$$

then we have

$$\lambda = \left(\frac{\epsilon_{3,1}}{\epsilon_{2,1}}\right)^{b_1} \cdots \left(\frac{\epsilon_{3,p}}{\epsilon_{2,p}}\right)^{b_p} \frac{1}{1+\zeta} - 1.$$

Since $|\zeta/(1+\zeta)| < 1$, arguing crudely, from (6·5), we have that $|\lambda| < 2^p\,|Y|^{1-p}$ and so

$$\log|\lambda| < p\,\log 2 - (p-1)\,\log|Y|. \tag{6·8}$$

It follows from (6·6) that $|\lambda| < 1/3$ whereby there exists $b_0 \in \mathbb{Z}$ with $|b_0| \leqslant (p+1)B$ such that, if we define a corresponding linear forms in logarithms

$$\Lambda = \left| b_0 \log(-1) + b_1 \log\left(\frac{\epsilon_{3,1}}{\epsilon_{2,1}}\right) + \cdots + b_p \log\left(\frac{\epsilon_{3,p}}{\epsilon_{2,p}}\right) - \log(\zeta+1) \right|,$$

we have $\Lambda \leqslant 2|\lambda|$.

To obtain a lower bound upon Λ (and hence $|\lambda|$), we will apply Theorem 3, arguing as in [**5**, section 9·3]. Suppressing the details, after some work we arrive at an inequality of the shape

$$\log|\lambda| > -2^{2p+16}\,p^{2p+11}\,\log\left(p^{3p}\,\log|Y|\right)\,(p!)^2\,R_K. \tag{6·9}$$

We apply [**5**, lemma 9·1] to bound the regulator R_K. If we suppose that we have $D_K \leqslant L$, then

$$R_K < \min\{f_K(L, 2 - t/1000)\ :\ t = 0, 1, \ldots, 999\},$$

where

$$f_K(L,s) = 2^{-1}\left(2^{1-p}\pi^{-p}\sqrt{L}\right)^s\,(\Gamma(s/2))^2\,(\Gamma(s))^{p-1}\,s^{2p+1}\,(s-1)^{1-2p}.$$

Since $D_K = 2^{4p-1}p^{2p}$, a short Maple computation reveals that, for $19 \leqslant p \leqslant 941$, we always have

$$\log R_K < 10458, \tag{6·10}$$

where the largest value of $\min\{f_K(L, 2 - t/1000)\ :\ t = 0, 1, \ldots, 999\}$ encountered corresponds to $p = 941$ and $t = 743$.

Combining (6·8), (6·9) and (6·10), we thus have

$$\log|Y| < 2^{2p+17}\,p^{2p+10}\,\log\left(p^{3p}\log|Y|\right)\,(p!)^2\exp(10458). \tag{6·11}$$

Since $p \leqslant 941$, in all cases we may conclude that $\log|Y| < 10^{15528}$, contradicting (6·6). We may thus conclude that $(1, \pm 1)$ are the only integer solutions to (2·1) for the primes p under consideration.

6·2. *Handling the values of* $3 \leqslant p \leqslant 17$

To finish the proof of Theorem 2, it remains to solve (2·1) for primes p with $3 \leqslant p \leqslant 17$, which we shall carry out in this subsection. Our strategy is to reduce the problem of treating equation (2·1) for a fixed odd prime p to that of solving (a finite collection of) Thue equations over $\mathbb{Z}$.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

As before, we write $\epsilon = 1 + \sqrt{2}$ for the fundamental unit of $\mathbb{Z}[\sqrt{2}]$ (the ring of integers of $\mathbb{Q}(\sqrt{2})$). Consider a solution (x, y, p) to (2·1) and write

$$z := (x^p + 3)/4, \tag{6·12}$$

so that the integers y and z satisfy

$$y^2 - 2z^2 = -1,$$

hence, as before (see (2·5)),

$$y + z\sqrt{2} = s\epsilon^k$$

for some odd integer k and $s \in \{-1, 1\}$. Replacing y by $-y$ leads to replacing k by $-k$ (see the proof of Lemma 4·6), so after possibly changing the sign of y we have

$$k \equiv s \pmod 4.$$

Writing

$$a + b\sqrt{2} = \epsilon^{\frac{k-1}{2}},$$

for $a, b \in \mathbb{Z}$, we have

$$a^2 - 2b^2 = (-1)^{\frac{k-1}{2}} = s \tag{6·13}$$

and

$$\begin{aligned} y + z\sqrt{2} &= s\epsilon(a + b\sqrt{2})^2 \\ &= s(a^2 + 4ab + 2b^2) + s(a^2 + 2ab + 2b^2)\sqrt{2}. \end{aligned}$$

Using this parametrisation for z together with (6·12) and (6·13), we have

$$\begin{aligned} sx^p &= 4sz - 3s \\ &= 4(a^2 + 2ab + 2b^2) - 3(a^2 - 2b^2) \\ &= a^2 + 8ab + 14b^2 \\ &= (a + 4b)^2 - 2b^2. \end{aligned}$$

Since a and p are odd, this implies that

$$(a + 4b) + b\sqrt{2} = \epsilon^t(u + v\sqrt{2})^p \tag{6·14}$$

for certain $u, v, t \in \mathbb{Z}$ with $|t| \leqslant (p - 1)/2$. Let us define binary forms over $\mathbb{Z}$ via

$$F_{p,t}(U, V) + G_{p,t}(U, V)\sqrt{2} = \epsilon^t(U + V\sqrt{2})^p$$

and

$$H_{p,t}(U, V) = (F_{p,t}(U, V) - 4G_{p,t}(U, V))^2 - 2G_{p,t}(U, V)^2.$$

Then (6·13) and (6·14) lead to

$$H_{p,t}(u, v) = s,$$

where $|u^2 - 2v^2| = |x|$. We have now reduced the solution of (2·1) for a fixed odd prime p to the solution of the $2p$ Thue equations of degree $2p$

$$H_{p,t}(U, V) = s, \quad U, V \in \mathbb{Z}, \quad t = 0, \pm 1, \ldots, \pm\frac{p-1}{2}, \quad s \in \{-1, 1\}. \tag{6·15}$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Table 1. (p, t, m) *for which* $H_{p,t}(U, V) \equiv 1 \pmod{m}$ *has no solutions.*

p	t	m
3	-1	7
3	1	3^2
5	$-2, -1, 2$	5^2
7	$-3, -2, -1, 2, 3$	7^2
7	$1, 3$	13
11	$-4, -1, 1, 3, 5$	11^2
11	$-5, -4, -3, -2, -1, 2, 3, 4, 5$	23
13	$-6, -4, -3, 4, 5$	79
13	$-5, -2, -1, 2, 3, 6$	313
17	$-8, \ldots, -1, 2, \ldots, 8$	103

Taking into account information from the modular method, namely Lemma 4·5, we can restrict to $s = 1$ when $p \geqslant 5$. If $p = 3$, then the three Thue equations in (6·15) corresponding to $s = -1$ can readily be seen to have no solutions; for $t = -1, 0, 1$ there are no solutions modulo 7, 9, 5 respectively. This means that for an odd prime p we only have to solve the p Thue equations

$$H_{p,t}(U, V) = 1, \quad U, V \in \mathbb{Z}, \quad t = 0, \pm 1, \ldots, \pm\frac{p-1}{2}. \tag{6·16}$$

If we define $h_{p,t}(x) = H_{p,t}(x, 1)$, let γ be a root of $h_{p,t}(x, 1) = 0$ and set $K = \mathbb{Q}(\gamma)$, then we have that the discriminant of K is $2^{p(6p-2)-1}p^{2p}$ and that K has precisely 2 real embeddings and hence p fundamental units.

We note that $H_{p,0}$ is monic in U, so the equation $H_{p,0}(U, V) = 1$ always has the solutions $U = \pm 1$, $V = 0$. If these are the only solutions to $H_{p,0}(U, V) = 1$ and the other $p - 1$ Thue equations in system (6·16) have no solutions, then it readily follows that $(x, y) = (1, \pm 1)$ are the only integer solution to (2·1) for our fixed odd prime p.

We restrict our attention to $3 \leqslant p \leqslant 17$. First of all, the Thue equation solver in `PARI/GP` [**15**] can (unconditionally) solve

$$H_{p,0}(U, V) = 1$$

for all these primes p rather quickly. The upshot of such a computation is that, apart from $(U, V) = (\pm 1, 0)$, there are no further solutions. Many of the other Thue equations in (6·16) can also be solved using `PARI/GP`. However, for some of the larger values of p and some values of t the computations appear to take a huge amount of time (and possibly memory). Luckily many of the Thue equations involved have local obstructions to solutions (which is something not automatically checked by `PARI/GP` when trying to solve the equations). In fact, the only pairs (p, t) with $3 \leqslant p \leqslant 17$ and $1 \leqslant |t| \leqslant (p-1)/2$ for which we cannot find a local obstruction for $H_{p,t}(U, V) = 1$ are given by

$$(p, t) \in \{(5, 1), (13, 1), (17, 1)\}.$$

For these pairs, we can in fact use the Thue equation solver in `PARI/GP` to show within reasonable time that $H_{p,t}(U, V) = 1$ has no integer solutions. For sake of completeness, for all (p, t) under consideration for which we found a local obstruction, we provide in Table 1 at least one modulus m such that the congruence $H_{p,t}(U, V) \equiv 1 \pmod{m}$ has no solutions.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Remark. It is not strictly necessary to invoke the modular method to deal with the odd primes $p \leqslant 17$. Most of the Thue equations in (6·15) with $s = -1$ can easily be solved, just like in the case when $p = 3$. In fact, for all odd primes $p \leqslant 17$ and all integers t with $|t| \leqslant (p-1)/2$ we can find a local obstruction for

$$H_{p,t}(U, V) = -1 \tag{6·17}$$

(although some of the moduli involved are much larger than those in Table 1), except when $(p, t) \in \{(13, -4), (13, 5)\}$. In the latter case the Thue equation solver in `PARI/GP` can show again that (6·17) has no solutions. For $(p, t) = (13, -4)$ we were not immediately able to solve (6·17). We did not pursue this however, but note instead that it seems possible to use the method of Chabauty-Coleman to deal completely with (2·1) for $p = 13$ without using the modular method; see below.

6·2·1. *Alternative approach to handling small p*

To solve (2·1) for a fixed odd prime p, without first reducing to Thue equations, we may note that this equation defines a hyperelliptic curve C_p of genus $p - 1$. Hence finding all integer or rational points on C_p would suffice. For convenience, consider the model for C_p in weighted projective space given by

$$C_p \ : \ 8y^2 = x^{2p} + 6x^p z^p + z^{2p}.$$

We want to show that $C_p(\mathbb{Q}) = \{(1 : \pm 1 : 1)\}$. We have the two (non-hyperelliptic) involutions on C_p

$$\iota_p^{\pm} : (x : y : z) \longmapsto (z : \pm y : x),$$

and their corresponding quotients

$$D_p^{\pm} := C_p/\iota_p^{\pm}.$$

A priori, for $p > 3$, it suffices to determine either $D_p^+(\mathbb{Q})$ or $D_p^-(\mathbb{Q})$ since D_p^+ and D_p^- are (hyperelliptic) curves of genus $(p - 1)/2 > 1$. For $p = 3$ it would suffice of course to find that at least one of $D_p^+(\mathbb{Q})$ or $D_p^-(\mathbb{Q})$ is finite.

To calculate explicit models for D_p^+ and D_p^-, we find the binary forms $F_p^{\pm}$ over $\mathbb{Z}$ of degree p such that

$$F_p^{\pm}(xz, (x \pm z)^2) = x^{2p} + 6x^p z^p + z^{2p}.$$

Introducing the variables

$$X^{\pm} := xz, \quad Y^{\pm} := (x \pm z)y, \quad Z^{\pm} := (x \pm z)^2,$$

we see that models for D_p^+ and D_p^- in weighted projective space are given by

$$D_p^{\pm} \ : \ 8Y^{\pm 2} = Z^{\pm} F_p^{\pm}(X^{\pm}, Z^{\pm}).$$

Furthermore, the rational points $(1 : \pm 1 : 1)$ on C_p map under ι_p^+ to $(1 : \pm 2 : 4)$ on D_p^+ and under ι_p^- to $(1 : 0 : 0)$ on D_p^-. We note that the point at infinity $(1 : 0 : 0)$ is also a rational point on D_p^+. It readily follows that if we can show that

$$D_p^+(\mathbb{Q}) = \{(1 : \pm 2 : 4), (1 : 0 : 0)\} \tag{6·18}$$

or

$$D_p^-(\mathbb{Q}) = \{(1 : 0 : 0)\}, \tag{6·19}$$

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

Table 2. *Upper bounds for ranks of the Jacobian of D_p^+ and D_p^-.*

p	3	5	7	11	13	17
Upper bound for rank(Jac(D_p^+)($\mathbb{Q}$))	1	1	1	2	1	2
Upper bound for rank(Jac(D_p^-)($\mathbb{Q}$))	0	0	1	1	1	2

then $C_p(\mathbb{Q}) = \{(1, \pm 1, 1)\}$ and consequently $(1, \pm 1)$ are the only integer solutions to (2·1) for the odd prime p under consideration.

Using `Magma`'s implementation of 2-descent on hyperelliptic Jacobians we obtain upper bounds for the $\mathbb{Q}$-ranks of Jac($D_p^{\pm}$) for several primes p; see Table 2. We see that the ranks of Jac(D_3^-)($\mathbb{Q}$) and Jac(D_5^-)($\mathbb{Q}$) are both 0. It is also easy to check that they both have trivial torsion. As a quick corollary we now obtain that (6·19) holds for $p = 3$ and $p = 5$. In fact (the Jacobian of) D_3^- is the elliptic curve with Cremona Reference $1728j1$; for D_3^+, the reference is $1728e1$. We can also easily check, for all primes p in Table (2), that (two of) the three obvious rational points on D_p^+ give rise to a non-torsion element on the Jacobian. We conclude that the ranks of Jac(D_7^+)($\mathbb{Q}$) and Jac(D_{13}^+)($\mathbb{Q}$) are both 1 and that for both of them we have an explicit generator for a subgroup of finite index. This means that it should be possible to use the method of Chabauty–Coleman to check that (6·18) holds for $p = 7$ and $p = 13$. Determining $C_p(\mathbb{Q})$ for $p = 11$ or $p \geqslant 17$ seems much harder.

7. *Frey Curves for shifted powers in more general Lucas sequences*

In this section, we will indicate how our preceding arguments fit into a more general framework. Let K be a real quadratic number field, $\mathcal{O}_K$ its ring of integers and $\epsilon \in \mathcal{O}_K$ a fundamental unit in K, with conjugate $\overline{\epsilon}$. Define the Lucas sequences, of the first and second kinds, respectively,

$$U_k = \frac{\epsilon^k - (\overline{\epsilon})^k}{\epsilon - \overline{\epsilon}} \quad \text{and} \quad V_k = \epsilon^k + (\overline{\epsilon})^k, \quad \text{for} \quad k \in \mathbb{Z}.$$

Let $a, c \in \mathbb{Q}$ with $a \neq 0$, and consider the problem of determining the shifted powers $ax^n + c$ in one of these sequences, i.e. determining all integers k, x and n with $n \geqslant 2$ such that we have

$$U_k = ax^n + c \tag{7·1}$$

or

$$V_k = ax^n + c. \tag{7·2}$$

If e.g. $\epsilon = (1 + \sqrt{5})/2$, this amounts to determining shifted powers in the Fibonacci (U_k) or Lucas (V_k) sequences. If $\epsilon = 1 + \sqrt{2}$, $(a, c) = (\pm 1/4, \pm 3/4)$ and k is odd, equation (7·1) corresponds to the main problem of this paper.

We will show that the arguments of this paper can potentially resolve such problems corresponding to either:

(i) equation (7·1) with k odd and Norm(ϵ) $= -1$; or

(ii) equation (7·2) with either k even or Norm(ϵ) $= 1$.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

We proceed from the observation that

$$\epsilon^k + \epsilon^{-k} \pm 2 = \begin{cases} \left(\epsilon^{k/2} \pm \epsilon^{-k/2}\right)^2 & \text{if } k \text{ is even,} \\ \epsilon\left(\epsilon^{\frac{k-1}{2}} \pm \epsilon^{\frac{-k-1}{2}}\right)^2 & \text{if } k \text{ is odd.} \end{cases} \tag{7·3}$$

If k is odd and $\mathrm{Norm}(\epsilon) = -1$, we have $(\overline{\epsilon})^k = -\epsilon^{-k}$ whereby

$$\left(\epsilon + \epsilon^{-1}\right) U_k \pm 2 = \epsilon\left(\epsilon^{\frac{k-1}{2}} \pm \epsilon^{\frac{-k-1}{2}}\right)^2.$$

It follows from equation (7·1) that

$$(\epsilon + \epsilon^{-1})ax^n + ((\epsilon + \epsilon^{-1})c \pm 2) = \epsilon\gamma_{k,\pm}^2, \tag{7·4}$$

where

$$\gamma_{k,\pm} := \epsilon^{\frac{k-1}{2}} \pm \epsilon^{\frac{-k-1}{2}} \in \mathcal{O}_K,$$

Similarly, if either k is even, or $\mathrm{Norm}(\epsilon) = 1$, we have

$$V_k = \epsilon^k + \epsilon^{-k},$$

and hence, from (7·3) and assuming that we have (7·2),

$$ax^n + (c \pm 2) = \begin{cases} \tau_{k,\pm}^2 & \text{if } k \text{ is even,} \\ \epsilon\gamma_{k,\pm}^2 & \text{if } k \text{ is odd,} \end{cases} \tag{7·5}$$

where

$$\tau_{k,\pm} := \epsilon^{k/2} \pm \epsilon^{-k/2} \in \mathcal{O}_K.$$

To either three term relation (7·4) or (7·5), we can actually associate several Frey curves – the most obvious are those corresponding to the generalized Fermat equations of signature $(n, n, 2)$ or signature $(n, 3, 2)$. Both these Frey curves are defined over the totally real number field K and therefore amenable to a Hilbert modular approach. In this setting, we can in fact generalize our choices of $a, c \in \mathbb{Q}$ to $a, c \in K$ and $x \in \mathbb{Z}$ to $x \in \mathcal{O}_K$.

Remark. If we also want to study (7·1) for k even or $\mathrm{Norm}(\epsilon) = 1$, or equation (7·2) when k is odd and $\mathrm{Norm}(\epsilon) = -1$, we can write down similar three term relations to those above, but now over $K(\sqrt{-1})$. The resulting Frey curves will therefore not *a priori* be defined over a totally real number field.

8. *Other applications*

In [**3**], equation (1·1) is solved in the case where $\{u_k\} = \{F_k\}$, the Fibonacci numbers and $c = \pm 1$. In this situation, the problem actually reduces to that of determining (almost) perfect powers in the Fibonacci and Lucas sequences (a program that is carried out in [**5**]; see also [**4**]), through a series of identities akin to

$$F_{4k} + 1 = F_{2k-1}L_{2k+1}.$$

Here, $\{L_k\}$ denotes the Lucas numbers, the companion sequence to the Fibonacci numbers. This reduction in case $c = \pm 1$ depends crucially upon the fact that

$$F_{-1} = F_1 = F_2 = 1 \text{ and } F_{-2} = -1,$$

and does not apparently extend to permit solution of the equation $F_k = ax^n + c$ for even a single fixed pair (a, c) with $|c| > 1$ (the case $c = -2$ is given as an open problem in [**3**]).

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

As explained in the preceding section, the methods of this paper potentially permit solution of $F_k = ax^n + c$ for any given pair (a, c) and *odd* values of the index k. For certain choices of c, however, the elementary arguments of [**3**] allow one to handle the remaining even index terms. By way of example, let us suppose that $c = F_{2j}$, for some integer j, so that

$$|c| \in \{1, 3, 8, 21, 55, 144, \ldots\}$$

whereby we are considering equations of the shape

$$F_k \pm F_{2j} = ax^n, \tag{8·1}$$

for given fixed a and j (here, k, x and n are variables). Then, appealing to the identity

$$F_i L_j = F_{i+j} + (-1)^j F_{i-j},$$

we have that

$$F_{4k} = F_{2k+j} L_{2k-j} + (-1)^{j+1} F_{2j}$$

and

$$F_{4k} = F_{2k-j} L_{2k+j} + (-1)^{j+1} F_{-2j} = F_{2k-j} L_{2k+j} + (-1)^j F_{2j}.$$

Assuming that we have $F_{4k} = ax^n + c$, if also j is even, say, it follows that

$$ax^n = F_{2k-j} L_{2k+j},$$

whilst if j is odd,

$$ax^n = F_{2k+j} L_{2k-j}.$$

Similarly, the identities

$$F_{4k+2} = F_{2k+j+1} L_{2k-j+1} + (-1)^j F_{2j}$$

and

$$F_{4k+2} = F_{2k-j+1} L_{2k+j+1} + (-1)^{j+1} F_{2j},$$

with $F_{4k+2} = ax^n + c$, imply that

$$ax^n = F_{2k+j+1} L_{2k-j+1} \text{ or } ax^n = F_{2k-j+1} L_{2k+j+1}.$$

In all cases, we are able to descend to a problem of (almost) perfect powers in the Fibonacci or Lucas sequences, one that has proven to be computationally tractable (whereby the same is potentially true for equation (8·1)).

Acknowledgements. The authors would like to thank the anonymous referee for a number of valuable suggestions which improved the paper.

REFERENCES

[**1**] M. A. BENNETT. Integer points on congruent number curves. *Int. J. Number Theory* **9** (2013), 1619–1640.

[**2**] W. BOSMA, J. CANNON and C. PLAYOUST. The Magma algebra system I: the user language. *J. Symb. Comp.* **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`.)

[**3**] Y. BUGEAUD, F. LUCA, M. MIGNOTTE and S. SIKSEK. Fibonacci numbers at most one away from a perfect power. *Elem. Math.* **63** (2008), 65–75.

[**4**] Y. BUGEAUD, F. LUCA, M. MIGNOTTE and S. SIKSEK. Almost powers in the Lucas sequences. *J. Théor. Nombres Bordeaux* **20** (2008), 555–600.

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press

[**5**] Y. BUGEAUD, M. MIGNOTTE and S. SIKSEK. Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers. *Ann. of Math.* **163** (2006), 969–1018.
[**6**] A. DAVID. Caractère d'isogénie et critères d'irréductibilité. arXiv:1103.3892v2 [math.NT].
[**7**] N. FREITAS, B. LE HUNG and S. SIKSEK. Elliptic curves over real quadratic fields are modular. *Invent. Math.* DOI 10.1007/s00222-014-0550-z.
[**8**] N. FREITAS and S. SIKSEK. An asymptotic Fermat's last theorem for five-sixths of real quadratic fields. *Compositio Math.* to appear.
[**9**] N. FREITAS and S. SIKSEK. Criteria for the irreducibility of mod p representations of Frey curves. *J. Théor. Nombres Bordeaux*, to appear.
[**10**] A. KRAUS and J. OESTERLÉ. Sur une question de B. Mazur. *Math. Ann.* **293** (2002), 259–275.
[**11**] M. LAURENT. Linear forms in two logarithms and interpolation determinants. II. *Acta Arith.* **133** (2008), 325–348.
[**12**] E. MATVEEV. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Math.* **64** (2000), 1217–1269.
[**13**] M. MIGNOTTE. A kit on linear forms in three logarithms, 45 pp, available at http://www-irma.u-strasbg.fr/~bugeaud/travaux/kit.ps.
[**14**] F. MOMOSE. Isogenies of prime degree over number fields. *Compositio Math.* **97** (1995), 329–348.
[**15**] THE PARI GROUP. PARI/GP version 2.7.0 (Bordeaux, 2014) http://pari.math.u-bordeaux.fr/.
[**16**] T. SHOREY and C. L. STEWART. Pure powers in recurrence sequences and some related Diophantine equations. *J. Number Theory* **27** (1987), 324–352.
[**17**] C. L. STEWART. On some Diophantine equations and related linear recurrence sequences. *Sém. de Théorie des Nombres, Paris* 1980–1981 (Birkhauser, Boston, 1982).

https://doi.org/10.1017/S0305004114000681 Published online by Cambridge University Press