Compositio Math. 142 (2006) 1103–1121
doi:10.1112/S0010437X06002181

Binomial Thue equations and polynomial powers

M. A. Bennett, K. Győry, M. Mignotte and Á. Pintér

Abstract

We explicitly solve a collection of binomial Thue equations with unknown degree and unknown S-unit coefficients, for a number of sets S of small cardinality. Equivalently, we characterize integers x such that the polynomial $x^2 + x$ assumes perfect power values, modulo S-units. These results are proved through a combination of techniques, including Frey curves and associated modular forms, lower bounds for linear forms in logarithms, the hypergeometric method of Thue and Siegel, local methods, and computational approaches to Thue equations of low degree. Along the way, we derive some new results on Fermat-type ternary equations, combining classical cyclotomy with Frey curve techniques.

1. Introduction

The binomial Thue equations

$$Ax^n - By^n = C, \tag{1.1}$$

where $n \geqslant 3$ and A, B and C are nonzero integers, play an important role in Diophantine analysis and have numerous applications; see, for example, [Mor69, ST86, Ben01, HSS01, Ben04, BGP04, GP05] and the references given there. It follows from a classical theorem of Thue [Thu09] that (1.1) has at most finitely many solutions in integers (x, y), which, via a result of Baker [Bak68], are explicitly bounded in size. If one allows $n \geqslant 3$ to be variable, Tijdeman [Tij75] showed that (1.1) has still at most finitely many solutions (x, y, n) with $|xy| > 1$ (and even that $\max\{x, y, n\}$ is effectively bounded). An extension of this result to the case where the coefficients A, B and C are, additionally, taken to be unknown S-units, rather than fixed, may be found in recent work of Győry, Pink and Pintér [GPP04]. Recall that, for a finite set of primes S, an integer a is called an S-unit if all its prime factors lie in S.

In the proofs of [Bak68], [Tij75] and [GPP04] Baker's theory of linear forms in logarithms was involved. Although the results of [Bak68] and [Tij75] have been improved several times, even the best known general upper bounds on the solutions of (1.1) are too large for numerical resolution of the equation in concrete cases.

Equation (1.1) with unknown $n \geqslant 3$ and unknown S-unit coefficients A, B has been resolved in only a few instances, in each case with $C = \pm 1$. For example, if $S = \{2\}$, the fact that (1.1) has no solution with $|xy| > 1$ is a consequence of work of Darmon and Merel [DM97] and Ribet [Rib97] on Fermat-type equations. For sets S of cardinality exceeding unity, the only explicit result known is Theorem 1.2 of [Ben04] which solves (1.1) for $C = \pm 1$ and $S = \{2, 3\}$. In the proof of this theorem, fundamental use is made of the fact that the primes 2 and 3 correspond to values of m for which one may construct Frey curves over $\mathbb{Q}$ from solutions (a, b, c) to $Aa^n + Bb^n = c^m$. However, for more

Received 13 July 2005, accepted in final form 24 March 2006.
2000 Mathematics Subject Classification 11D45, 11D61 (primary), 11J82, 11J86 (secondary).
Keywords: binomial Thue equations, superelliptic equations, explicit resolution.
The first author was supported in part by a grant from NSERC. The second author was supported in part by grants T38225 and T42985 from the HNFSR. The fourth author was supported in part by grants F34981 and T42985 from the HNFSR.

general sets S, even those with $|S| = 2$, additional arguments and new ingredients are also needed, including improved lower bounds for linear forms in three (or, potentially, more) logarithms.

Our first result concerning (1.1) generalizes the aforementioned earlier work with $S \subseteq \{2, 3\}$.

Theorem 1.1. *Let $S = \{p, q\}$ for p and q primes with $2 \leqslant p, q \leqslant 13$. If A, B, x, y and n are positive integers with A, B S-units, $A < B$ and $n \geqslant 3$, then the only solutions to (1.1) with $C = \pm 1$ are those with*

$$n \geqslant 3, \quad A \in \{1, 2, 3, 4, 7, 8\}, \quad x = y = 1$$

and

$$\begin{gathered} n = 3, \quad (A, x) = (1, 2), (1, 3), (1, 4), (1, 9), (1, 19), (1, 23), (3, 2), (5, 11), \\ n = 4, \quad (A, x) = (1, 2), (1, 3), (1, 5), (3, 2), \\ n = 5, \quad (A, x) = (1, 2), (1, 3), \\ n = 6, \quad (A, x) = (1, 2). \end{gathered}$$

Another classical Diophantine problem, given a polynomial $f(x)$ with integer coefficients and a finite set S of primes, is to determine the integers x for which the superelliptic equation

$$f(x) = \omega y^n \tag{1.2}$$

has solutions in integers y, ω with ω an S-unit. As is well-known, (1.2) may be reduced to a number of equations of the shape (1.1) over the splitting field of f. When $n \geqslant 3$ is fixed and f has at least two simple zeros, an explicit upper bound was given for the solutions x, y, ω of (1.2) by Baker [Bak69]. This result was extended in [ST76, Tur82, ST86, GPP04] to the case when n is also unknown, but with exceptionally large bounds for x and y.

Unfortunately, it is virtually always an impractical task to actually compute the solutions of (1.2) for a given polynomial and set of primes. In the case when $f(x) = x(x + 1)$, however, (1.2) and (1.1) with $C = \pm 1$ and A, B unknown integer S-units are equivalent. In this situation, the aforementioned results of [DM97, Rib97, Ben04] concerning (1.1) furnish all the solutions to (1.2) for $S = \{2, 3\}$.

Our Theorem 1.1 is equivalent to the following result.

Theorem 1.2. *Let S be as in Theorem 1.1, and let $f(x) = x(x + 1)$. If x is a positive integer such that (1.2) has solutions in integers y, n and ω with ω an S-unit and $n \geqslant 3$, then*

$$x \in \{1, 2, 3, 4, 7, 8, 15, 24, 26, 27, 32, 48, 63, 64, 80, 242, 624, 728, 6655, 6859, 12\,167\}.$$

We note that, for the polynomial $f(x) = x(x + 1)$, there is no loss of generality in restricting to positive values of x, since $f(-x) = f(x - 1)$.

One of the main interests in our theorems is that their proofs require a combination of information derived from (several) Frey curves with the hypergeometric method of Thue and Siegel, recent lower bounds for linear forms in three logarithms, the use of somewhat involved local considerations, and techniques for solving Thue equations of moderate degree, based on ideas of Hanrot [Han97]. For a number of the sets S under consideration (such as $S = \{2, 5\}$ or $\{2, 7\}$), it is only through careful application of state-of-the-art estimates, together with this hybrid Frey-curve approach, that we are able to completely solve (1.1) and (1.2).

The outline of this paper is as follows. In proving Theorem 1.1, we restrict ourselves to those solutions of (1.1) for which $xy > 1$. The solutions with $x = y = 1$ will be given at the end of the proof. In Section 2, we establish two new results (Theorems 2.1 and 2.2) on general ternary equations, based on the modularity of Galois representations, to determine the solutions of (1.1) for all but small n,

except for $S = \{2, 5\}$ and $\{2, 7\}$. In Section 3, we appeal to lower bounds for linear forms in logarithms to bound n in these latter two cases. Section 4 is comprised of two new results (Theorems 4.1 and 4.2) on generalized Fermat-type equations, combining work from the classical theory of cyclotomic fields with techniques based on the modularity of Frey curves. For our purposes, these results are used primarily to reduce considerably our remaining computations. Sections 5 and 6 deal with local (and not-so-local!) methods for proving that (1.1) has no solution if $S = \{2, 5\}$ or $\{2, 7\}$, except for small n. Finally, in Sections 7 and 8, we conclude by treating the remaining small values of n and the solutions $x = y = 1$, respectively.

We note that our Theorems 2.1, 2.2, 4.1 and 4.2 concerning ternary equations may be of independent interest.

2. Ternary equations via Frey curves

For $S = \{p, q\}$ with distinct primes $2 \leqslant p, q \leqslant 13$, we will consider those positive integer solutions A, B, x, y, n of (1.1) for which $xy > 1$, where we take $C = 1$, and suppose that A and B are S-units. Our first step is to obtain a reasonable upper bound for n. To achieve this, we will begin by considering more general equations of the form

$$AX^n - BY^n = Z^m, \quad m \in \{3, n\}.$$

Approaches to solving such equations, analogous to that employed by Wiles [Wil95] to prove Fermat's last theorem, may be found in numerous recent papers, for example, [BS04, BVY04, DM97, Kra97, Rib97, Ser87].

For our purposes, we will restrict attention to the cases $m = 3$ and $m = n$. If $2 \notin S$, we will appeal to the following theorem.

THEOREM 2.1. *Suppose that $AB = p^\alpha q^\beta$ where either $p, q \in \{3, 5, 7, 11, 13\}$. If $n > 7$ is prime and coprime to pq, then the equation*

$$AX^n - BY^n = Z^3 \tag{2.1}$$

has no solutions in integers (X, Y, Z) with $|XY| > 1$, XY even, and AX, BY and Z pairwise coprime.

In other words, under the assumptions of Theorem 2.1, (2.1) has no solutions with $|XY| > 1$ and Z odd.

Proof. If one of p or q, say p, is equal to 3 and $\beta \equiv 0 \pmod{n}$, then this is a special case of [BVY04, Theorem 1.5]. Otherwise, let us suppose that we have a solution to (2.1) in integers (X, Y, Z) with $|XY| > 1$, XY even, and AX, BY and Z pairwise coprime. Without loss of generality, we may assume that $AX \not\equiv 0 \pmod{3}$ and $BY^n \not\equiv 1 \pmod{3}$, and that A and B are nth power free. Following [DM97, BVY04], we consider the elliptic curve

$$E : y^2 + 3Zxy - BY^n y = x^3. \tag{2.2}$$

By what are now fairly standard arguments (see, e.g., [BVY04] or [DM97]), the canonical Galois representation

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n),$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $E[n]$ of E, may be shown, for $n > 7$ prime, to arise from a weight 2, level $N_n(E)$ cuspidal new form

$$f = \sum_{r=1}^{\infty} c_r \exp(2r\pi iz)$$

of trivial Nebentypus character. Here,

$$N_n(E) = \begin{cases} \mathrm{rad}_3(AB)\varepsilon_3 & \text{if } n \nmid AB, \\ n\,\mathrm{rad}_3(AB)\varepsilon_3 & \text{if } n \mid AB, \end{cases}$$

where

$$\varepsilon_3 = \begin{cases} 1, & \text{if } \mathrm{ord}_3(B) = 3, \\ 3, & \text{if } \mathrm{ord}_3(BY^n) \geqslant 4 \text{ and } \mathrm{ord}_3(B) \neq 3, \\ 9, & \text{if } 9 \mid (2 - BY^n - 3Z), \\ 27, & \text{if } 3 \parallel (2 - BY^n - 3Z) \text{ or if } \mathrm{ord}_3(B) = 2, \\ 81, & \text{if } \mathrm{ord}_3(B) = 1, \end{cases}$$

and $\mathrm{rad}_l(m)$ denotes the product of distinct prime factors of m which are different from l.

For our purposes, what is useful about this result is that, writing K_f for the field of definition of the Fourier coefficients c_r of the putative form f, and supposing that l is a prime, coprime to $nN_n(E)$, we necessarily have

$$\mathrm{Norm}_{K_f/\mathbb{Q}}(c_l - a_l) \equiv 0 \pmod{n}, \tag{2.3}$$

where $a_l = \pm(l+1)$ (if $l \mid XY$), or

$$a_l \in \{x \in \mathbb{Z} : |x| < 2\sqrt{l}, x \equiv l + 1 \pmod 3\} \quad (\text{if } l \text{ is coprime to } XY).$$

This is Proposition 4.2 of [BVY04]; the congruence conditions upon the a_l arise from the fact that our Frey curve E has a rational 3-isogeny.

To prove Theorem 2.1, it is enough to show that no modular forms with the properties stated here can, in fact, exist. If

$$N_n(E) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\},$$

then there are no weight 2 cuspidal newforms whatsoever at level $N_n(E)$, whence we derive an immediate contradiction. Otherwise, the crucial observation to make is that, from the assumption that XY is even, we have $a_2 = \pm 3$, whereby, from (2.3), either

$$c_2 \equiv 3 \pmod{\nu} \quad \text{or} \quad c_2 \equiv -3 \pmod{\nu}, \tag{2.4}$$

for a prime ν of K_f, lying above n. If f is one-dimensional (so that it corresponds to an elliptic curve over $\mathbb{Q}$), since $N_n(E)$ is always odd when $2 \notin S$, we necessarily have $c_2 \in \{0, \pm 1, \pm 2\}$, contradicting both congruences in (2.4) for $n > 7$. For higher dimensional forms, either of (2.4) fixes c_l modulo ν, for each l coprime to $nN_n(E)$. From Stein's Modular Forms Database [Ste], we check that, for the levels $N_n(E)$ of interest, in all cases, we may find at least one l contradicting (2.3). By way of example, to discount the possibility of the form $(819, 11)$ (in Stein's notation) giving rise to a solution to (2.1), with $n = 11$ or $n \geqslant 17$ prime, we note that the Fourier coefficients for this form lie in the number field $\mathbb{Q}(\theta)$, where $\theta^4 - 7\theta^2 + 4 = 0$. Since $c_2 = \theta$, both congruences in (2.4) lead to the conclusion that $n = 11$. From $c_5 = -\theta^3/2 + 7\theta/2$, $c_{17} = 2\theta$ and $c_{19} = \theta^2 + 1$, we are unable to use (2.3) to eliminate the possibility that $n = 11$ by using $l \in \{5, 17, 19\}$. Happily though, we have $c_{23} = -3\theta^3/2 + 13\theta/2$ and, hence,

$$c_{23} \equiv \pm 21 \equiv \pm 1 \pmod{\nu}$$

for ν a prime above 11 in $\mathbb{Q}(\theta)$. Since

$$a_{23} \in \{0, \pm 3, \pm 6, \pm 9, \pm 24\},$$

this contradicts (2.3). Arguing similarly for all forms at the levels $N_n(E)$ under consideration, completes the proof of Theorem 2.1. In the following table, we list the $N_n(E)$ of importance, together with the c_l employed in our proof.

p	q	$N_n(E)$	c_l
3	5	$15, 45, 135, 405$	c_2, c_7
3	7	$21, 63, 189, 567$	c_2, c_5
3	11	$11, 33, 99, 297, 891$	c_2, c_5
3	13	$39, 117, 351, 1053$	c_2, c_5, c_7, c_{17}
5	7	$105, 315, 945$	$c_2, c_{11}, c_{13}, c_{17}$
5	11	$165, 495, 1485$	c_2, c_7
5	13	$195, 585, 1755$	c_2, c_7
7	11	$231, 693, 2079$	c_2, c_5, c_{17}
7	13	$273, 819, 2457$	c_2, c_5, c_{11}, c_{23}
11	13	$429, 1287, 3861$	c_2, c_5

□

The next result will be of use in case $2 \in S$.

THEOREM 2.2. *Suppose that $AB = 2^\alpha q^\beta$ where $q \in \{3, 5, 7, 11, 13\}$. If $n > 7$ is a prime, coprime to q, then the equation*

$$AX^n - BY^n = Z^n \tag{2.5}$$

has no solutions in integers (X, Y, Z) with $|XY| > 1$ and AX, BY and Z pairwise coprime, unless, possibly,

$$(q, \alpha) \in \{(3,1), (3,2), (3,3), (5,2), (5,3), (7,2), (7,3)\} \quad \textit{and } XY \textit{ is odd}$$

or

$$(q, n, \alpha) \in \{(11, 7, 1), (13, 7, \alpha)\} \quad \textit{and } XY \textit{ is odd.}$$

This implies that if, in particular, $n > 13$ is prime and $\alpha = 0$ or $\alpha \geqslant 4$, then (2.5) has no solutions with $|XY| > 1$. For $n > 13$, this can be compared with the corresponding results of [Ben04, Rib97, Ser87, Wil95].

Proof. If either $\alpha \equiv 0 \pmod n$ or $\beta \equiv 0 \pmod n$, this follows from work of Darmon and Merel [DM97], Ribet [Rib97], Serre [Ser87] and Wiles [Wil95]. Otherwise, supposing that n is coprime to $\alpha\beta$, we may assume, without loss of generality, that $AX^n \equiv -1 \pmod 4$ and $BY \equiv 0 \pmod 2$, and consider

$$E : y^2 = x(x - AX^n)(x - BY^n).$$

As in the preceding proof, the canonical Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $E[n]$ of E, may be shown, for $n > 7$ prime, to arise from a weight 2, level $N_n(E)$ cuspidal new form

$$f = \sum_{r=1}^{\infty} c_r \exp(2r\pi i z)$$

of trivial Nebentypus character (see, e.g., [Kra97]). Here,

$$N_n(E) = \begin{cases} \mathrm{rad}_2(AB)\varepsilon_n & \text{if } n \nmid AB, \\ n\,\mathrm{rad}_2(AB)\varepsilon_n & \text{if } n \mid AB, \end{cases}$$

where

$$\varepsilon_n = \begin{cases} 1, & \text{if } \mathrm{ord}_2(B) = 4, \\ 2, & \text{if } \mathrm{ord}_2(B) \geqslant 5, \\ 8, & \text{if } \mathrm{ord}_2(B) = 2 \text{ or } 3, \\ 32, & \text{if } \mathrm{ord}_2(B) = 1. \end{cases}$$

If $N_n(E) \in \{3, 5, 6, 7, 10, 13, 22\}$ then there are no weight 2 cuspidal newforms at these levels.

As previously, we have (2.3) for each prime l, coprime to $nN_n(E)$, where now $a_l = \pm(l+1)$ (if $l \mid XY$), or

$$a_l \in \{x \in \mathbb{Z} : |x| < 2\sqrt{l}, x \equiv l + 1 \,(\mathrm{mod}\ 4)\} \quad (\text{if } l \text{ is coprime to } XY).$$

Once again, from Stein's Modular Forms Database [Ste], we may check that (2.3) leads to a contradiction for all prime n under consideration, by choosing $l \in \{3, 5\}$ as noted in the following table.

q	$N_n(E)$	c_l
5	160	c_3
7	14, 224	c_3
11	11, 88, 352	c_3, c_5
13	26, 104, 416	c_3, c_5

In the exceptional cases it is easy to show that XY must be odd. Indeed, if XY is even and, for example $q = 7$, (2.5) reduces to the case of conductor 14, where a useful fact is that elliptic curves over $\mathbb{Q}$ with conductor 14 do not have full 2-rational torsion. In the other cases we can argue similarly to prove the assertion. □

From Theorems 2.1 and 2.2, and [Ben04, Theorem 1.2] to complete the proof of Theorem 1.1 with $xy > 1$, it remains to treat (1.1) for $C = \pm 1$ with

$$\text{either } n \in \{3, 4, 5, 7\} \quad \text{or} \quad n \in \{11, 13\} \text{ and } n \mid AB, \tag{2.6}$$

as well as to show that, for primes $n \geqslant 11$, the following equations have no solutions in integers X, Y with $|XY| > 1$ and odd

$$X^n - 2^\alpha 5^\beta Y^n = 1, \quad 2 \leqslant \alpha \leqslant 3, 1 \leqslant \beta \leqslant n-1, \tag{2.7}$$

$$X^n - 2^\alpha 7^\beta Y^n = 1, \quad 2 \leqslant \alpha \leqslant 3, 1 \leqslant \beta \leqslant n-1, \tag{2.8}$$

$$2^\alpha X^n - 5^\beta Y^n = 1, \quad 2 \leqslant \alpha \leqslant 3, 1 \leqslant \beta \leqslant n-1, \tag{2.9}$$

and

$$2^\alpha X^n - 7^\beta Y^n = 1, \quad 2 \leqslant \alpha \leqslant 3, 1 \leqslant \beta \leqslant n-1. \tag{2.10}$$

In Sections 3–6, we will deal with these last four equations. The cases listed in (2.6) will be treated in Section 7.

3. Linear forms in logarithms

To find an upper bound for n in (2.7), (2.8), (2.9) and (2.10), for *fixed* α and β, we may apply a result derived from lower bounds for linear forms in two complex logarithms, say as follows.

Proposition 3.1. *Let α_1 and α_2 be multiplicatively independent positive rational numbers, suppose that b_1 and b_2 are positive integers, and define*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1.$$

Let a_1, a_2, h, k and $\rho_2 > 1$ be positive real numbers, and set $\lambda = \log \rho_2$. Suppose that

$$h \geqslant \log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\lambda + f(K) + 0.023,$$
$$a_i \geqslant \max\{1, \rho_2|\log\alpha_i| - \log(\alpha_i) + 2h(\alpha_i)\} \quad (i = 1, 2), \quad \text{and} \quad a_1a_2 \geqslant \lambda^2,$$

where

$$f(x) = \log\left(\frac{(1+\sqrt{x-1})\sqrt{x}}{x-1}\right) + \frac{\log x}{6x(x-1)} + \frac{3}{2} + \log\left(\frac{3}{4}\right) + \frac{\log(x/(x-1))}{x-1},$$

$L = 2 + [2h/\lambda]$, and $K = 1 + [kLa_1a_2]$. Here, if p and q are positive integers, $h(p/q) = \log\max\{p, q\}$. Then, if k satisfies the inequality

$$3(L-1)\lambda k - 3hk - L\sqrt{k} - \frac{1}{a_1} - \frac{1}{a_2} - 2\sqrt{\frac{L}{a_1a_2}} \geqslant 0, \tag{3.1}$$

it follows that

$$\log|\Lambda| \geqslant -\lambda k L^2 a_1 a_2 - \max\{\lambda(L-0.5) + \log((L^{3/2} + L^2\sqrt{k})\max\{a_1, a_2\} + L), \log 2\}.$$

This is Theorem 1.5 of [Mig98], a variant of Théorème 2 of Laurent, Mignotte, and Nesterenko [LMN95]. We will apply this later théorème to handle certain 'degenerate' linear forms in three logarithms. It will also prove convenient to state the following corollary of this result.

Proposition 3.2. *Let A, B and n be positive integers with $n \geqslant 3$ and $A > B$. If there exist integers X and Y with $|XY| > 1$ and*

$$AX^n - BY^n = 1,$$

then

$$n \leqslant 3106\log A.$$

Proof. This has been proved by iterated application of Proposition 3.1; see [Pin]. □

Unfortunately, there is no obvious way to bound β, independent of n. To deal with (2.7), (2.8), (2.9) and (2.10), we will thus appeal to a lower bound for linear forms in *three* complex logarithms. The strongest such result available until recently was due to Matveev [Mat00]. Unfortunately, for our purposes, the bounds implicit in [Mat00] are not strong enough to enable us to complete the proof of Theorem 1.1. We thus must apply a more recent bound, due to Mignotte [Mig, Proposition 5.1], which is in fact a special case of an improvement of Theorem 12.9 in [BMS]. Even after specializing this result to the problem at hand, we warn the reader that it remains extremely technical to state!

Proposition 3.3. *Let α_1, α_2 and α_3 be multiplicatively independent rational numbers with $\alpha_i > 1$ for $1 \leqslant i \leqslant 3$, suppose that b_1, b_2 and b_3 are positive coprime (not necessarily pairwise) rational integers and define*

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

Write

$$d_1 = \gcd(b_1, b_2), \quad d_3 = \gcd(b_3, b_2), \quad b_1 = d_1b_1', \quad b_2 = d_1b_2' = d_3b_2'', \quad b_3 = d_3b_3'',$$

and let $\rho_3 \geqslant e$ be a real number and $\lambda = \log\rho_3$. Choose a_1, a_2 and a_3 to be real numbers such that

$$a_i \geqslant (\rho_3 - 1)\log\alpha_i + 2h(\alpha_i), \quad i = 1, 2, 3,$$

and assume further that

$$\Omega = a_1a_2a_3 \geqslant 2.5 \quad \text{and} \quad a = \min\{a_1, a_2, a_3\} \geqslant 0.62.$$

Let m and χ be real numbers with $m \geqslant 3$ and $0 < \chi \leqslant 2$, and $L \geqslant 5$ an integer. Define

$$K = [m\Omega L], \quad c_1 = \max\{(\chi mL)^{2/3}, \sqrt{2mL/a}\},$$
$$c_2 = \max\{2^{1/3}(mL)^{2/3}, \sqrt{m/a}L\}, \quad c_3 = (6m^2)^{1/3}L,$$
$$R_i = [c_i a_2 a_3], \quad S_i = [c_i a_1 a_3] \quad \text{and} \quad T_i = [c_i a_1 a_2],$$

for $1 \leqslant i \leqslant 3$. Let us also write

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

and define

$$C = \max\left\{\frac{R}{a_2a_3}, \frac{S}{a_1a_3}, \frac{T}{a_1a_2}\right\} \quad \text{and} \quad V = ((R_1+1)(S_1+1)(T_1+1))^{1/2}.$$

Finally, assume that

$$\kappa\lambda - 2\log(KL) - 3gCL\Omega - (K-1)\log\tilde{b} + 2\log 1.36 \geqslant 0, \tag{3.2}$$

where

$$\kappa = \frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L}, \quad g = \frac{1}{4} - \frac{K^2L}{12RST}$$

and

$$\tilde{b} = e^3\left(\frac{C\Omega}{2K}\right)^2\left(\frac{b_1'}{a_2} + \frac{b_2'}{a_1}\right)\left(\frac{b_3''}{a_2} + \frac{b_2''}{a_3}\right).$$

Then either

$$\log|\Lambda| > -(KL + \log(3KL))\lambda,$$

or at least one of the following conditions (C1), (C2), (C3) holds:

(Ci) *$|b_1| \leqslant R_i, |b_2| \leqslant S_i$ and $|b_3| \leqslant T_i$ for $i = 1, 2$; or*

(C3) *either there exist nonzero rational integers r_0 and s_0 such that*

$$r_0b_2 = s_0b_1$$

with

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

where

$$M = \max\{R_1 + S_1 + 1,\ S_1 + T_1 + 1,\ R_1 + T_1 + 1,\ \chi V\},$$

or there exist rational integers r_1, s_1, t_1 and t_2, with $r_1s_1 \neq 0$, such that

$$(t_1b_1 + r_1b_3)s_1 = r_1b_2t_2, \quad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1, \quad \gcd(r_1, s_1) = \delta,$$
$$|r_1s_1| \leqslant \delta \cdot \frac{(R_1+1)(S_1+1)}{M - \max\{R_1, S_1\}}, \quad |s_1t_1| \leqslant \delta \cdot \frac{(S_1+1)(T_1+1)}{M - \max\{S_1, T_1\}}$$

and

$$|r_1t_2| \leqslant \delta \cdot \frac{(R_1+1)(T_1+1)}{M - \max\{R_1, T_1\}}.$$

In essence, this result provides a nice lower bound on the linear form Λ, unless there is a 'small' linear dependency amongst the coefficients b_i (these are just the conditions (C1), (C2) and (C3)). To apply this bound to (2.7), (2.8), (2.9) and (2.10), it will be helpful to have a decent lower bound for $|X|$ and $|Y|$ at hand.

LEMMA 3.4. *Let $n > 7$ be prime. Suppose that X and Y are odd integers with $|XY| > 1$, satisfying one of the equations (2.7), (2.8). Then*

$$|X| > \exp\{n/3106\} - 1.$$

If X and Y are odd integers with $|XY| > 1$, satisfying one of the equations (2.9), (2.10), then

$$|X| > n - 2\sqrt{n} + 1.$$

Proof. Suppose first that there exist odd integers X and Y with $|XY| > 1$, satisfying one of the equations (2.7), (2.8). Rewriting these equations as

$$\left(\frac{X^n - 1}{X - 1}\right)(X - 1) = 2^\alpha q^\beta Y^n \quad \text{with } q = 5 \text{ or } 7,$$

we note that any prime divisor of $(X^n - 1)/(X - 1)$ may be readily shown to be congruent to 0 or 1 modulo n. It follows that $2^\alpha q^\beta$ divides $X - 1$ and, hence,

$$|X - 1| \geqslant 2^\alpha q^\beta.$$

However, Proposition 3.2 implies that

$$n < 3106 \log(2^\alpha q^\beta) \leqslant 3106 \log(|X - 1|),$$

whereby

$$|X| > \exp\{n/3106\} - 1.$$

If, on the other hand, there exist odd integers X and Y with $|XY| > 1$, satisfying one of the equations (2.9), (2.10), then we consider the elliptic curve

$$E : y^2 = x(x + q^\beta Y^n)(x + 2^\alpha X^n), q \in \{5, 7\}.$$

As in the proof of Theorem 2.2, the corresponding mod n Galois representation arises from a weight 2 cuspidal newform of level 40 or 56, depending on whether $q = 5$ or 7, respectively. Since $|XY| > 1$, either $n \mid X$ (so that $|X| \geqslant n$) or there exists a prime l, coprime to $2qn$, such that $l \mid X$. In the latter case, E has multiplicative reduction at l and, hence, from (2.3) and the fact that all weight 2 newforms at levels 40 and 56 are one-dimensional, we have

$$n \mid c_l \pm (l + 1),$$

where c_l is a rational integer with (via the Hasse–Weil bounds) $|c_l| < 2\sqrt{l}$. It follows that

$$n < l + 2\sqrt{l} + 1 \leqslant |X| + 2\sqrt{|X|} + 1,$$

whence $|X| > n - 2\sqrt{n} + 1$. □

Carefully combining the previous results in this sections yields the following bounds on n in (2.7), (2.8), (2.9) and (2.10).

PROPOSITION 3.5. *If there exist odd integers X and Y with $|XY| > 1$, satisfying one of the equations (2.7), (2.8), (2.9), (2.10), then $n < n_0$ in the following table.*

Equation	n_0
(2.7)	4.4×10^7
(2.8)	5.5×10^7
(2.9)	5.9×10^7
(2.10)	7.8×10^7

Proof. We will restrict our attention to, for example, (2.9), where, for added simplicity, we will assume that X and Y are positive. The other cases are proved in a very similar fashion; the stronger

estimates for (2.7) and (2.8) are the result of the correspondingly sharper lower bounds upon X, from Lemma 3.4. If we have positive integers X and Y with $XY > 1$ satisfying (2.9), then necessarily $X > Y \geqslant 1$ (since, via Proposition 3.2, we may assume that $\beta > 2$). We consider the linear form

$$\Lambda = \beta \log 5 - n \log(X/Y) - \alpha \log 2.$$

In the notation of Proposition 3.3, we have

$$\alpha_1 = X/Y, \quad \alpha_2 = 5, \quad \alpha_3 = 2, \quad b_1 = n, \quad b_2 = \beta \quad \text{and} \quad b_3 = \alpha.$$

It follows from (2.9) that $|e^{\Lambda} - 1| \leqslant 2^{-5}$. Hence,

$$|\Lambda| \leqslant 2|e^{\Lambda} - 1| = 2\left|\frac{5^{\beta}}{2^{\alpha}}\left(\frac{Y}{X}\right)^{n} - 1\right| \leqslant 2X^{-n}. \tag{3.3}$$

Suppose, here and henceforth, that

$$n \geqslant 5.9 \times 10^7,$$

whence, by Lemma 3.4, $X > 5.89 \times 10^7$. We will apply Proposition 3.3 with

$$\chi = 1/2, \quad L = 73, \quad m = 28, \quad \rho_3 = 7.3,$$
$$a_1 = 6.3 \log 5 + 2 \log X, \quad a_2 = 8.3 \log 5, \quad \text{and} \quad a = a_3 = 8.3 \log 2,$$

whereby

$$c_1 = 101.4613408\ldots, \quad c_2 = 202.9226816\ldots, \quad \text{and} \quad c_3 = 1223.1469343\ldots$$

Using these constants, we have

$$R_1 = 7797, \quad R_2 = 15\,595, \quad R_3 = 94\,001,$$

and, from the fact that $X > 5.89 \times 10^7$,

$$S_1 \leqslant [1498.2467 \log X],$$
$$S_2 \leqslant [2996.4934 \log X], \quad S_3 \leqslant [18\,061.8138 \log X],$$
$$T_1 \leqslant [3478.8211 \log X], \quad T_2 \leqslant [6957.6422 \log X], \quad \text{and} \quad T_3 \leqslant [41\,938.2329 \log X].$$

It is easy to verify that

$$\chi V \geqslant \max\{R_1 + S_1 + 1, S_1 + T_1 + 1, R_1 + T_1 + 1\},$$
$$B_S := \frac{(R_1+1)(T_1+1)}{\chi V - \max\{R_1, T_1\}} < 279, \quad B_T := \frac{(R_1+1)(S_1+1)}{\chi V - \max\{R_1, S_1\}} < 118,$$

independently of X (for $X > 5.89 \times 10^7$), and that inequality (3.2) is satisfied.

We thus have either

$$\log|\Lambda| \geqslant -KL \log \rho_3 - \log(3KL) > -5.851 \times 10^7 \log X,$$

whence, with (3.3),

$$n < 5.9 \times 10^7,$$

or one of conditions (C1), (C2) or (C3). In cases (C1) or (C2), we in fact obtain the stronger inequality

$$n \leqslant \max\{R_1, R_2\} = 15\,595,$$

contradicting $n \geqslant 5.9 \times 10^7$. Moreover, the first case of condition (C3), that is, $r_0 b_2 = s_0 b_1$, cannot hold because of the bound on r_0 (namely $|r_0| \leqslant B_S$) and the fact that $b_1 = n \geqslant 5.9 \times 10^7$ is prime, and $b_2 = \beta < n$. On supposing that condition (C3) holds, then we necessarily have

$$s_1 t_1 n + r_1 s_1 \alpha - r_1 t_2 \beta = 0,$$

where r_1, s_1, t_1 and t_2 are as in the statement of Proposition 3.3. We write $r_1 = \delta r'$ and $s_1 = \delta s'$, whence

$$s't_1 n + \delta r' s' \alpha - r' t_2 \beta = 0.$$

It follows that $r' \mid n$ and, hence, since $|\delta r' s'| \leqslant B_T < 118$ and $n \geqslant 5.9 \times 10^7$ is prime, $r' = \pm 1$. Without loss of generality, we may thus write

$$s't_1 n + \delta s' \alpha - t_2 \beta = 0. \tag{3.4}$$

Since $2 \leqslant \alpha \leqslant 3$, $1 \leqslant \beta \leqslant n-1$ and $|\delta s'| \leqslant 117$, this implies

$$|s't_1| \leqslant |t_2| \leqslant B_S < 279.$$

Now the identity (3.4) enables us to rewrite $t_2\Lambda$ as a linear form in two logarithms. In our example,

$$t_2\Lambda = n \log(5^{s't_1} \times (Y/X)^{t_2}) - \alpha \log(2^{t_2} \times 5^{-\delta s'}).$$

Note that (3.4), together with the inequalities

$$2 \leqslant |\delta s' \alpha| \leqslant 351 \quad \text{and} \quad n > 5.9 \times 10^7,$$

imply that $t_2 \neq 0$. Without loss of generality, we may in fact assume, from (3.4), that t_2 and $s't_1$ are positive integers.

We will apply Proposition 3.1 with, in the notation of that result,

$$\alpha_1 = 2^{t_2} \times 5^{-s'\delta}, \quad \alpha_2 = 5^{s't_1} \times (Y/X)^{t_2}, \quad b_1 = \alpha \quad \text{and} \quad b_2 = n.$$

Note that

$$\log \alpha_2 = s't_1 \log 5 - t_2 \log(X/Y)$$

and so, from (3.4),

$$n \log \alpha_2 = t_2(\beta \log 5 - n \log(X/Y)) - \delta s' \alpha \log 5.$$

Combining this with (3.3), it follows that

$$n \log \alpha_2 = t_2(\alpha \log 2 + 2\theta X^{-n}) - \delta s' \alpha \log 5,$$

where $|\theta| < 1$. This implies, from the inequalities $n > 5.9 \times 10^7$, $2 \leqslant \alpha \leqslant 3$, $|\delta s'| \leqslant 117$, $t_2 < 279$ and $X > 5.89 \times 10^7$, that

$$|\log \alpha_2| < 0.0001.$$

Choosing $\rho_2 = 12$ therefore enables us to take

$$a_1 = 13 \log(2^{t_2} \times 5^{|s'\delta|}), \quad a_2 = 2t_2 \log X + 0.01, \quad h = \log n,$$

and

$$0.029 < k < 0.035,$$

chosen as small as possible, while satisfying inequality (3.1). With these choices, for $1 \leqslant |s'\delta| \leqslant 117$ and $1 \leqslant t_2 \leqslant 278$, we verify, in each case, that Proposition 3.1 and inequality (3.3) together imply that $n < 5.9 \times 10^7$, as desired. Arguing similarly for the remaining equations completes the proof of Proposition 3.5. □

4. Cyclotomy

One may reasonably approach (2.7) and (2.8) via classical work on cyclotomic fields. With this in mind, let B be a nonzero rational integer, and consider the equation

$$X^n + Y^n = BZ^n, \tag{4.1}$$

where $n > 3$ and X, Y, Z are coprime nonzero rational integers. Let $\phi(B)$ denote Euler's function. We have the following results, which may be of independent interest.

Theorem 4.1. *Let $n > 3$ be a prime and B a positive integer such that n is coprime to $B\phi(B)$, and*

$$B^{n-1} \not\equiv 2^{n-1} \pmod{n^2}. \tag{4.2}$$

Suppose that (4.1) has a solution in pairwise relatively prime nonzero integers X, Y and Z. Then either (i) $n \mid Z$ or (ii) $n \mid XY$, BZ is odd and $r^{n-1} \equiv 1 \pmod{n^2}$ for each divisor r of B. Further, in either case (i) or (ii), we have

$$\log n < 3R \log R, \quad \text{where } R = \text{rad } (B) = \prod_{p \mid B} p. \tag{4.3}$$

This is a sharper and rather more explicit version of a recent result of Halberstadt and Kraus [HK02, Theorem. 6.1]. Apart from (4.3), Theorem 4.1 was proved in [BGP04] (see also [Gyo66]). If we have that $n \mid XYZ$ in (4.1), it is easy to show that we necessarily have (4.3), with no additional hypotheses on n and B.

Proof. If B is a perfect nth power this is an immediate consequence of [Wil95]. Otherwise, the result is a consequence (cf. in [BGP04, Corollary 6.2]) of Satz 1 of Győry [Gyo66], except for the inequality for n. We note that the proofs in [Gyo66] depend on Eisenstein's reciprocity theorem in cyclomotic fields. To derive an upper bound for n, in the case $n \mid XYZ$, we argue as in Kraus [Kra97]. As in the proof of our Theorem 2.2, we associate to a nontrivial solution of (4.1) (noting that the case $B = 2$ was treated in [DM97]) a Frey curve E with corresponding weight 2 cuspidal newform f of level N dividing $16R$. If this newform is one-dimensional and n fails to divide B, then E has multiplicative reduction at n, while f corresponds to an elliptic curve $F/\mathbb{Q}$ with good reduction at n. By Proposition 3 of Kraus and Oesterlé [KO92], it follows that the nth Fourier coefficient a_n of the curve F satisfies

$$a_n \equiv \pm(n+1) \equiv \pm 1 \pmod{n}.$$

Since a_n is an even rational integer, satisfying $|a_n| < 2\sqrt{n}$, this is a contradiction.

It remains to treat the case where our cuspidal newform $f = \sum_{r=1}^{\infty} c_r \exp(2r\pi iz)$ at level N has coefficients in a number field of degree at least 2. Via Lemme 1 of [Kra97], if we define

$$\mu(N) = N \prod_{l \mid N} \left(1 + \frac{1}{l}\right),$$

where l runs through the distinct prime factors of N, then there necessarily exists a prime p, coprime to N, such that $c_p \notin \mathbb{Z}$, with $p \leqslant \mu(N)/6$. From (2.3), it follows that n divides the (nonzero) integer

$$\text{Norm}_{K_f/\mathbb{Q}}(c_p \pm a_p),$$

and, hence, via the Hasse–Weil bounds,

$$n \leqslant (p + 1 + 2\sqrt{p})^{[K_f:\mathbb{Q}]}.$$

Since a result of Martin [Mar05] yields the inequality

$$[K_f : \mathbb{Q}] \leqslant \frac{N+1}{12},$$

and we have $p \leqslant \mu(N)/6$, it follows that

$$n \leqslant (\sqrt{\mu(N)/6} + 1)^{(N+1)/6}. \tag{4.4}$$

Assume that B is even; the case where B is odd leads to a stronger bound via a similar analysis. From the fact that N divides $16R$, the last inequality implies that

$$\mu(N) \leqslant 24R \prod_{l|B, l\neq 2} \left(1+\frac{1}{l}\right) \leqslant 24R \prod_{l|B, l\neq 2} \left(1-\frac{1}{l}\right)^{-1}$$

and so

$$\mu(N) \leqslant 24R \frac{\mathrm{rad}_2(B)}{\phi(\mathrm{rad}_2(B))},$$

where $\mathrm{rad}_2(B) = \prod_{l|B, l\neq 2} l$. Applying Lemma 25 of [Mar05] to give an explicit lower bound for $\phi(\mathrm{rad}_2(B))$, we conclude that

$$\mu(N) \leqslant 24R \frac{\log R}{\log 2}$$

and, hence, from (4.4),

$$n \leqslant \left(2\left(R\frac{\log R}{\log 2}\right)^{1/2} + 1\right)^{(16R+1)/6}.$$

This implies the stated bound as soon as $R \geqslant 10$. For $R \in \{2,3,5,7\}$, Theorem 4.1 (in much stronger form) is a consequence of work of Serre [Ser87] and Ribet [Rib97]. Finally, if $R = 6$, the fact that all weight 2, level $N = 2^\alpha \cdot 3$ cuspidal newforms are one-dimensional, for $\alpha \in \{0,1,3,5\}$, leads to the desired conclusion. □

Our second result of this section will prove helpful in Section 7, treating (1.1) for $n \in \{11, 13\}$, $A = 1$, $n \mid B$ and $C = \pm 1$. Where this result is applicable, it is much more computationally efficient than solving the corresponding Thue equations via linear forms in logarithms and lattice basis reduction.

Let $n > 3$ be a prime, and suppose that in (4.1) B is divisible by n. Let $n, p_1, \ldots, p_r$ denote the distinct prime factors of B, and, for $r \geqslant 1$, $f_1, \ldots, f_r$ the smallest positive integers for which

$$p_i^{f_i} \equiv 1 \pmod{n}, \quad i = 1, \ldots, r.$$

Set $\mathrm{ord}_n(B) = N$, and $\zeta = e^{2\pi i/n}$. Denote by h_0 the class number of the number field $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$, and by B_m the mth Bernoulli number. We recall that $B_{2m+1} = 0$ for $m \geqslant 1$.

THEOREM 4.2. *Suppose that $N = 1$ or $N \geqslant 4$, and that the following conditions hold:*

(i) *h_0 is not divisible by n;*

(ii) *none of the Bernoulli numbers $B_{2tn}, t = 1, \ldots, (n-3)/2$, is divisible by n^3;*

(iii) *if $r \geqslant 1$,*

$$\sum_{i=1}^{r} \frac{1}{f_i} \leqslant \frac{n-3}{2(n-1)}$$

and $(n-1)/f_i$ is odd for $i = 1, \ldots, r$.

Then (4.1) has no solution in coprime nonzero rational integers X, Y, Z which are not divisible by n.

In the particular case $n \mid N$, Theorem 4.2 was proved in [Ago77, Theorem 2], (see also [Gan72], where the proof of the corresponding result is not correct). Theorem 2 of [Ago77] is stated with $2 \mid f_i$ in place of $2 \nmid ((n-1)/f_i)$ for $i = 1, \ldots r$. However, the proof in [Ago77] is correct and complete only under the stronger assumption $2 \nmid ((n-1)/f_i)$.

We note that condition (i) is satisfied by all odd primes $n < 5500$ (cf. [BS72]) while a simple check using Pari shows that condition (ii) is satisfied by all odd primes $n < 350$.

Proof. Suppose that (4.1) has a solution in coprime nonzero rational integers X, Y and Z not divisible by n. Then it follows that $n \mid X + Y$ and

$$n \mid (X^n + Y^n)/(X + Y)$$

whence $N \geqslant 4$.

We shall prove more. Let M be a positive integer with $M \leqslant (n-1)/2$ or $M \geqslant (3n+1)/2$. Further, let $\kappa = (1-\zeta)(1-\zeta^{-1})$ and suppose that δ is a nonzero algebraic integer in K_0 having at most $(n-3)/2$ distinct prime ideal factors in $K = \mathbb{Q}(\zeta)$, each of which is real. We show that under assumptions (i) and (ii), the equation

$$X^n + Y^n = \eta \kappa^M \delta Z^n \tag{4.5}$$

where η is a unit in K_0, is impossible in pairwise relatively prime nonzero integers X, Y, Z in K_0 which are not divisible by the prime element $\lambda = 1 - \zeta$ in K.

Indeed, (4.5) implies that λ divides $X + \zeta^i Y$ in K for each i with $0 \leqslant i \leqslant n-1$. However, $\kappa = \mu\lambda^2$ for a unit μ in K, and hence the inequality $M \leqslant (n-1)/2$ cannot hold. For $M \geqslant (3n+1)/2$, our claim can be proved in the same way as the corresponding assertion was proved in [Ago77] in the particular case $M = mn$ with $m > 1$. It suffices to take M everywhere in [Ago77] in place of mn, and observe that the congruences for α on [Ago77, p. 5] are valid not only modulo λ^{M-2n}, but also modulo λ^{M-n-1}.

Consider again (4.1). We have $n = \eta_0 \kappa^{(n-1)/2}$ with some unit η_0 in K_0. Putting $\eta = \eta_0^N, M = N(n-1)/2$ and $\delta = B/n^N$, every solution of (4.1) in coprime nonzero rational integers X, Y, Z not divisible by n yields a solution of (4.5). Further, by using condition (iii) one can prove (see, e.g., [Ago77, p. 6]) that δ has at most $(n-3)/2$ distinct real prime ideal factors in K. Now the assertion follows from our above result concerning (4.5). □

5. Local approaches to (2.7) and (2.8)

Consider first (2.7) and (2.8) for $n < 7.8 \times 10^7$. Using Theorem 4.1 we show that, for given n and α, β is uniquely determinable. This will be crucial for solving (2.7) and (2.8). By applying Theorem 4.1 to (2.7) and (2.8) with $B = 2^\alpha q^\beta$, for $\alpha \in \{2, 3\}$, and $q \in \{5, 7\}$, we conclude that either $n \mid Y$, or that

$$(2^\alpha q^\beta)^{n-1} \equiv 2^{n-1} \pmod{n^2},$$

and, thus,

$$(2^{\alpha-1} q^\beta)^{n-1} \equiv 1 \pmod{n^2}, \tag{5.1}$$

where $q = 5$ and 7, respectively, and $\alpha \in \{2, 3\}$, $1 \leqslant \beta \leqslant n-1$.

If $n \mid Y$, then we may argue as in the proof of Theorem 4.1. The fact that all weight 2 cuspidal newforms at levels 40 and 56 are one-dimensional (corresponding to elliptic curves over $\mathbb{Q}$ with rational 2-torsion) leads to a contradiction. It remains therefore to treat those α, β and n satisfying congruence (5.1). We begin by showing that, for fixed α, q and $n \leqslant 4 \times 10^{12}$, (5.1) has a single solution in $0 < \beta < n$. Let g be a primitive root mod n^2, and t_q, t_2 be positive rational integers with $\max\{t_q, t_2\} < n(n-1)$ such that

$$g^{t_q} \equiv q \pmod{n^2} \quad \text{and} \quad g^{t_2} \equiv 2 \pmod{n^2}.$$

From (5.1), we have

$$(g^{\beta t_q + (\alpha-1)t_2})^{n-1} \equiv 1 \pmod{n^2}$$

and so

$$\beta t_q + (\alpha - 1) t_2 \equiv 0 \pmod{n}. \tag{5.2}$$

If $n \mid t_2 t_q$, then $n \mid t_2$ and $n \mid t_q$, whence

$$2^{n-1} \equiv q^{n-1} \equiv 1 \pmod{n^2}.$$

However, from [CDP97], the only primes n for which $2^{n-1} \equiv 1 \pmod{n^2}$ and $n \leqslant 4 \times 10^{12}$ are $n = 1093$ and $n = 3511$. In neither case do we have $5^{n-1} \equiv 1 \pmod{n^2}$ or $7^{n-1} \equiv 1 \pmod{n^2}$, hence this is a contradiction for $n \leqslant 4 \times 10^{12}$. Otherwise, if n is coprime to $t_2 t_q$, then (5.2) has a unique integral solution β in the interval $(0, n)$.

We will use this information to reduce considerably the calculations involved in proving that for $n \geqslant 11$ prime, (2.7) and (2.8) have no solutions in integers X and Y, with $|XY| > 1$.

To complete the proof that the only integer solutions to (2.7) and (2.8) are with $|XY| \leqslant 1$, we will begin by arguing locally, finding, for each (α, β, q, n), a prime l such that $l \mid Y$. This will guarantee that our Frey curve corresponding to a solution to (2.7) or (2.8) has multiplicative reduction at l, which, in turn, will lead us to a contradiction. This method was applied to similar problems by the first author in [Ben04].

We begin with (2.7). For each prime n with $11 \leqslant n < 4.4 \times 10^7$, each $\alpha \in \{2, 3\}$ and, as we saw above, the unique $\beta = \beta(\alpha, n)$ satisfying (5.1) with $q = 5$, we consider (2.7) modulo various primes $l \equiv 1 \pmod{n}$. There are

$$2\pi(4.4 \times 10^7) - 8 = 5\,322\,760$$

such triples (α, β, n) to treat. If $l = 2kn + 1$ for suitably small k, relative to n, then we might reasonably hope that, from (2.7), necessarily $l \mid Y$. If this occurs, it follows that our corresponding Frey curve has multiplicative reduction at l, whence, for an elliptic curve $F/\mathbb{Q}$ of conductor 40, the lth Fourier coefficient c_l satisfies

$$c_l \equiv \pm(l + 1) \equiv \pm 2 \pmod{n}. \tag{5.3}$$

If k is not too large, the Hasse–Weil bounds thus imply that $c_l = \pm 2$.

We wrote a simple program in Pari GP to find, for each (α, β, n) under consideration, a prime l for which $l \mid Y$, but c_l fails to satisfy (5.3). This took only a few minutes on an old Sun Sparc. For example, if say $n = 10\,000\,019$ and $\alpha = 2$, we find that 6 is a primitive root modulo n^2, that

$$t_2 = 18\,273\,596\,511\,709, \quad t_5 = 54\,085\,373\,386\,760$$

and, hence, $\beta = 3\,015\,935$. Next, we choose $l = 80\,000\,153$ and note that, if l fails to divide XY, then

$$X^n, Y^n \equiv \pm 1, \pm 538\,808, \pm 6\,494\,373, \pm 13\,435\,164 \pmod{l}. \tag{5.4}$$

It follows that

$$X^{10\,000\,019} - 4 \cdot 5^{3\,015\,935} Y^{10\,000\,019} \not\equiv 1 \pmod{l},$$

unless $l \mid XY$. However, the lth Fourier coefficient for an elliptic curve of conductor 40 satisfies $c_{80\,000\,153} = -16\,470$, contradicting (5.3). This shows that (2.7) has no solution with $\alpha = 2$, $n = 10\,000\,019$ and $|XY| > 1$.

We argue in a similar fashion for (2.8), only now dealing with primes $n < 5.5 \times 10^7$. This leads us to

$$2\pi(5.5 \times 10^7) - 8 = 6\,564\,392$$

triples (α, β, n). As before, for each of these, we find a prime l with the desired properties. This completes the proof that (2.7) and (2.8) have no solutions with $|XY| > 1$, for $n \geqslant 11$ prime. Details of these computations are available from the first author on request.

6. Local approaches to (2.9) and (2.10)

In the case of (2.9) and (2.10), as in the previous section, we consider the equations modulo primes l of the form $l = 2kn + 1$. The terms X^n and Y^n assume only $2k + 1$ values modulo l and, hence, (2.9) and (2.10), viewed modulo l, restrict β to lie in a (small) subset $S_{\alpha,q,n,l}$ of $\{1, 2, \dots, n-1\}$. Choosing a second prime $l_1 = 2k_1 n + 1$, $l_1 > l$, we might be so lucky that

$$S_{\alpha,q,n,l} \cap S_{\alpha,q,n,l_1}$$

is empty. For $(\alpha, q) = (2, 5)$ or $(3, 7)$, however, this cannot occur, since

$$1 \in S_{2,5,n,l} \quad \text{and} \quad 1 \in S_{3,7,n,l},$$

for all n and l. Our best hope for these cases, then, would be to find primes l and l_1 such that

$$S_{\alpha,q,n,l} \cap S_{\alpha,q,n,l_1} = \{1\}.$$

As it transpires, for each $n > 19$, $\alpha \in \{2, 3\}$ and $q \in \{5, 7\}$, we are able to find pairs l and l_1 such that

$$S_{\alpha,q,n,l} \cap S_{\alpha,q,n,l_1} = \emptyset, \quad \text{if } (\alpha, q) \in \{(3, 5), (2, 7)\},$$

or

$$S_{\alpha,q,n,l} \cap S_{\alpha,q,n,l_1} = \{1\}, \quad \text{if } (\alpha, q) \in \{(2, 5), (3, 7)\}.$$

By way of example, if $\alpha = 2$, $n = 10\,000\,019$, and we have a solution to (2.9), then, setting $l = 80\,000\,153$, either $l \mid XY$ (which we saw in the previous section to be impossible) or we have (5.4). It follows that

$$\beta \in \{1, 228\,430, 834\,421, 1\,282\,074, 2\,092\,402, 3\,736\,215, 5\,753\,495, 6\,834\,596\}. \tag{6.1}$$

Now consider (2.9) modulo $l_1 = 380\,000\,723$. For an elliptic curve over $\mathbb{Q}$ of conductor 40, we have $c_{l_1} = 29\,280$ and, hence, we may suppose that l_1 is coprime to XY. Thus, we have that X^n and Y^n are congruent modulo l_1 to one of

$$\begin{aligned} &\pm 1, \pm 82\,112\,813, \pm 149\,954\,656, \pm 79\,032\,476, \pm 110\,277\,417, \pm 135\,718\,056, \pm 18\,775\,479, \\ &\pm 140\,828\,911, \pm 97\,873\,722, \pm 132\,355\,249, \pm 170\,198\,844, \pm 71\,588\,544, \pm 275\,744\,734, \\ &\pm 2\,816\,836, \pm 41\,375\,381, \pm 84\,539\,473, \pm 172\,217\,362, \pm 92\,827\,353, \pm 100\,960\,138. \end{aligned}$$

It follows that

$$\begin{aligned} \beta \in \{&1, 211\,982, 348\,127, 519\,850, 536\,141, 835\,642, 916\,539, 966\,752, 1\,000\,154, 1\,267\,974, \\ &1\,377\,872, 1\,964\,604, 2\,857\,367, 4\,438\,428, 4\,679\,933, 5\,509\,457, 5\,520\,173, 5\,600\,982, \\ &5\,856\,938, 6\,078\,164, 6\,122\,024, 6\,209\,295, 6\,555\,956, 6\,768\,172, 7\,433\,870, 7\,516\,082, \\ &7\,905\,690, 7\,983\,714, 8\,159\,851, 8\,296\,491, 8\,301\,055, 8\,516\,044, 8\,601\,690, 8\,641\,726, \\ &9\,058\,277, 9\,391\,416, 9\,413\,209, 9\,487\,924\}, \end{aligned}$$

and, hence, with (6.1), that $\beta = 1$.

After a reasonably short calculation, it remains, for $n > 19$, to handle the cases $\beta = 1$ where $(\alpha, q) = (2, 5)$ and $(3, 7)$, that is, the equations

$$4X^n - 5Y^n = 1 \quad \text{and} \quad 8X^n - 7Y^n = 1. \tag{6.2}$$

We appeal to a result of the first author [Ben01, Theorem 1.2].

Proposition 6.1. *If A, B and n are integers with $AB \neq 0$ and $n \geqslant 3$, then the equation*

$$|AX^n - BY^n| = 1$$

has at most one solution in positive rational integers X and Y.

From this, it follows that the equations in (6.2) have no solutions in integers X, Y with $|XY| > 1$.

In a number of cases, with $11 \leqslant n \leqslant 19$, the techniques of this section are apparently insufficient to handle the corresponding Diophantine equations (2.9) and (2.10). In particular, this is the case for

$$(\alpha, \beta, q, n) \in \{(2,5,5,11), (2,7,5,13), (3,9,5,17), (2,15,5,19), \\ (3,9,5,19), (3,17,5,19), (2,3,7,19), (3,3,7,19)\}. \tag{6.3}$$

To treat these and the other remaining equations with n small, we turn to recent computational work, combining lower bounds for linear forms in logarithms with techniques for rapid calculation of systems of independent units in number fields, and lattice-basis reduction algorithms.

7. Computational Thue equations

To complete the proof of Theorem 1.1 in the case $xy > 1$, it remains to treat a number of equations of type (1.1) with reasonably small values of n ($n \leqslant 19$, in fact). Namely, it suffices to solve (1.1) with $C = \pm 1$ for the n listed in (2.6), and (2.9) and (2.10) for (α, β, q, n) given in (6.3). As a first step, we considerably reduced the number of equations to be solved. When $1 < A < B$, we used local arguments to solve the many equations under consideration. In the case $A = 1, n \in \{11, 13\}, n \mid B$, we very quickly solved 784 of the equations in question by means of Theorem 4.2. Namely, we showed that if $\beta \notin \{2, 3\}$, then the equations

$$x^{11} - p^{\alpha} 11^{\beta} y^{11} = \pm 1 \quad \text{for } p \in \{2, 7, 13\}, 11 \nmid \beta,$$

and

$$x^{13} - p^{\alpha} 13^{\beta} y^{13} = \pm 1 \quad \text{for } p \in \{2, 5, 7, 11\}, 13 \nmid \beta,$$

have no solutions in nonnegative integers x, y, α, β with $xy > 1$.

For $n \leqslant 7$, it was reasonably routine to solve by Pari the remaining equations. For slightly larger n, however, obtaining an unconditional result (i.e. one that does not depend on the generalized Riemann hypothesis) remains a difficult problem. To deal with our remaining equations, for $11 \leqslant n \leqslant 19$, we are very grateful to Hanrot, who wrote an extension of Pari, Version 2.2.8 (development Changes-1.1035), which contains a new treatment of Thue equations based on his paper [Han97]. In this paper, he shows that the knowledge of a subgroup of finite index in the full group of units is actually sufficient to solve a Thue equation (the principal bottleneck of the classical algorithm, currently, is the computation of the unit group of the field). With this new software, we can solve Thue equations of rather large degree in a reasonable time. Without Hanrot's new method, we would have failed to solve many of these equations. A reasonably short (although nontrivial) computation thus completes the proof of Theorem 1.1, in case $xy > 1$.

8. Solutions of (1.1) with $x = y = 1$

Finally, let us suppose that we have a solution to (1.1) with $x = y = 1, C = \pm 1$ and A, B unknown S-units, for $S = \{p, q\}, 2 \leqslant p < q \leqslant 13$. It follows that $p = 2$ and, hence, we necessarily have

$$2^{\alpha} - q^{\beta} = \pm 1, \quad \text{for } q \in \{3, 5, 7, 11, 13\}$$

and α, β nonnegative integers. Via Mihailescu [Mih04] (a hammer for a fly, in this case), we have that $\min\{\alpha, \beta\} \leqslant 1$, unless $(\alpha, \beta, q) = (3, 2, 3)$. It is easy to check that these solutions correspond to the values $x \leqslant 8$ in the statement of Theorem 1.2. This completes our proof.

9. Concluding remarks

The techniques of this paper may also be extended with suitable perseverance to other two-element sets S. The cases treated in Theorems 1.1 and 1.2 are adequate, however, to illustrate our methods.

Acknowledgement

The authors are indebted to the referees for their valuable and helpful remarks, and for pointing out some inaccuracies in an earlier version of the paper.

References

Ago77 T. Agoh, *On the Diophantine equation concerning Fermat's last theorem*, TRU Math. **13** (1977), 1–8.

Bak68 A. Baker, *Contributions to the theory of Diophantine equations. I, II*, Philos. Trans. Roy. Soc. London **263** (1968), 173–191, 193–208.

Bak69 A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

Ben01 M. A. Bennett, *Rational approximation to algebraic numbers of small height: the Diophantine equation* $|ax^n - by^n| = 1$, J. reine angew. Math. **535** (2001), 1–49.

Ben04 M. A. Bennett, *Products of consecutive integers*, Bull. London Math. Soc. **36** (2004), 683–694.

BGP04 M. A. Bennett, K. Győry and Á. Pintér, *On the Diophantine equation* $1^k + 2^k + \cdots + x^k = y^n$, Compositio Math. **140** (2004), 1417–1431.

BS04 M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.

BVY04 M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compositio Math. **140** (2004), 1399–1416.

BS72 Z. I. Borevich and I. R. Shafarevich, *Number theory* (Russian), second edition (Izdat. Nauka, Moscow, 1972).

BMS Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), 969–1018.

CDP97 R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449.

DM97 H. Darmon and L. Merel, *Winding quotient and some variants of Fermat's last theorem*, J. reine angew. Math. **490** (1997), 81–100.

Gan72 J. M. Gandhi, *On generalized Fermat's last theorem II*, J. reine angew. Math. **256** (1972), 163–167.

Gyo66 K. Győry, *Über die diophantische Gleichung* $x^p + y^p = cz^p$, Publ. Math. Debrecen **13** (1966), 301–305.

GPP04 K. Győry, I. Pink and A. Pintér, *Power values of polynomials and binomial Thue–Mahler equations*, Publ. Math. Debrecen **65** (2004), 342–362.

GP05 K. Győry and Á. Pintér, *Almost perfect powers in products of consecutive integers*, Monatsh. Math. **145** (2005), 19–33.

HK02 E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. reine angew. Math. **548** (2002), 167–234.

Han97 G. Hanrot, *Solving Thue equations without the full unit group*, Math. Comp. **69** (1997), 395–405.

HSS01 G. Hanrot, N. Saradha and T. N. Shorey, *Almost perfect powers in consecutive integers*, Acta Arith. **99** (2001), 13–25.

Kra97 A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), 1139–1161.

KO92 A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

LMN95 M. Laurent, M. Mignotte and Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 285–321.

Mar05 G. Martin, *Dimensions of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, J. Number Theory **112** (2005), 298–331.

Mat00 E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. (Engl. transl. Izv. Math. **64** (2000), 1217–1269.)

Mig98 M. Mignotte, *A corollary to a theorem of Laurent–Mignotte–Nesterenko*, Acta Arith. **86** (1998), 101–111.

Mig M. Mignotte, *A kit of linear forms in three logarithms*, Publ. Inst. Rech. Math. Av. (Strasbourg), to appear.

Mih04 P. Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. reine angew. Math. **572** (2004), 167–195.

Mor69 L. J. Mordell, *Diophantine equations* (Academic Press, London, 1969).

Pin Á. Pintér, *On the power values of power sums*, to appear.

Rib97 K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. **79** (1997), 7–16.

ST76 A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. **31** (1976), 199–204.

Ser87 J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

ST86 T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations* (Cambridge University Press, Cambridge, 1986).

Ste W. Stein, *Modular forms database*, http://modular.fas.harvard.edu/Tables/.

Thu09 A. Thue, *Über Annäherungenswerte algebraischer Zahlen*, J. reine angew. Math. **135** (1909), 284–305.

Tij75 R. Tijdeman, *Some applications of Baker's sharpened bounds to Diophantine equations*, Séminaire Delange–Pisot–Poitou, 1974/1975, exp. 24 (Secrétariat Mathématique, Paris, 1975).

Tur82 J. Turk, *Polynomial values and almost powers*, Michigan Math. J. **29** (1982), 213–220.

Wil95 A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551.

M. A. Bennett bennett@math.ubc.ca
Department of Mathematics, University of British Columbia, Vancouver BC, Canada

K. Győry gyory@math.klte.hu
Mathematical Institute, Number Theory Research Group of the Hungarian Academy of Sciences, University of Debrecen, Debrecen, Hungary

M. Mignotte mignotte@math.u-strasbg.fr
Department of Mathematics, University of Strasbourg, Strasbourg, France

Á. Pintér apinter@math.klte.hu
Mathematical Institute, Number Theory Research Group of the Hungarian Academy of Sciences, University of Debrecen, Debrecen, Hungary