Publ. Math. Debrecen
70/3-4 (2007), 483–501

On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$, I

By K. GYŐRY (Debrecen) and Á. PINTÉR (Debrecen)

Abstract. In our paper we initiate a systematic treatment for solving the title equation for bounded positive integer coefficients A, B and C. To illustrate our approach we explicitly solve the equation in integers x, y and n with $|xy| > 1$, $n \geq 3$ for a collection of coefficients A, B, C. We first derive, for concrete values of $A, B, C \leq 100$, a relatively small upper bound for n, provided that the equation under consideration has no solution with $|xy| \leq 1$ (cf. Theorem 1). Then we give among others all the solutions (x, y, n) for $C = 1$, $A, B \leq 20$ (cf. Theorem 3), and for $A = C = 1$, $B \leq 70$ (cf. Theorem 4). Our method, which may, with some effort, be extended to larger values of A, B and C, combines a wide variety of techniques, classical and modern, in Diophantine analysis.

1. Introduction

Many problems in number theory can be reduced to Diophantine equations of the form

$$|Ax^n - By^n| = C, \tag{1}$$

where A, B and C are positive integers with

$$1 \leq A < B \quad \text{and} \quad \gcd(A, B) = 1, \tag{2}$$

x, y are unknown integers and $n \geq 3$ is either fixed or also unknown; see e.g. [18], [22], [2], [14], [3], [5], [12], [6] and the references given there. As is known,

Mathematics Subject Classification: Primary: 11D45, 11D61; Secondary: 11D41, 11J82, 11J86.
Key words and phrases: Diophantine equations, binomial Thue-equations, exponential equations, resolution of equations.
The first author was supported in part by grants T38225 and T42985 from the HNFSR. The second author was supported by grants T42985 and T48791 from the HNFSR.

for fixed n equation (1) possesses at most finitely many solutions in integers (x, y), and these are explicitly bounded in size; cf. [25] and [1]. Moreover, in the case when n is also unknown, TIJDEMAN [26] showed that $\max\{|x|, |y|, n\}$ is still effectively bounded for every integer solution (x, y, n) with $|xy| > 1$ and $n \geq 3$. This effective finiteness result has been extended in [11] to the more general situation when, for a finite set of primes S, the numbers A, B, C are unknown S-units rather than fixed, that is all prime factors of A, B and C lie in S.

In the proofs of [1], [26] and [11] the theory of logarithmic forms was involved. The upper bounds obtained in [1] and [26] on the solutions have been improved several times, but even the best known bounds are too large for the resolution of (1) in concrete cases. To actually compute the solutions several other methods are also needed.

Equation (1) with unknown $n \geq 3$ has been resolved in only a few instances, in each case with $C = 1$. Then BENNETT [2] showed by means of the hypergeometric method that for $B = A + 1$, equation (1) has no solution with $|xy| > 1$. In [3], [5] and [20], (1) has been explicitly solved for some choices of the coefficients (A, B). For certain sets of primes S, all the solutions of equation (1) with S-unit coefficients A, B have been determined. Namely, if $S = \{2\}$, it is a consequence of work of DARMON and MEREL [9] and RIBET [21] on Fermat-type equations that (1) has no solution with $|xy| > 1$. For $S = \{2, 3\}$, all solutions of (1) are given in [3]. Recently, this result has been extended in [6] to the case when $S = \{p, q\}$ for p and q primes with $2 \leq p$, $q \leq 13$;* see also [8] where (1) is solved for $C = 1$, $A = p^\alpha$, $B = q^\beta$ with primes $p < q \leq 31$.

The proofs in [3], [5], [6], [8] and [20] require a combination of virtually every technique in modern Diophantine analysis, including local methods, some classical results in cyclotomic fields, lower bounds for linear forms in logarithms of algebraic numbers, computational methods for finding the solutions to Thue equations of small degree, the hypergeometric method, and results on ternary equations based on Galois representations and modular forms.

The purpose of the present paper is to initiate a systematic treatment of solving equations of the form (1) with bounded coefficients. Combining the aforementioned methods and techniques with some results of [2], [5], [6], [20] and with certain new ideas, we solve explicitly a collection of equations (1) in unknown integers (x, y, n) with $n \geq 3$, where A, B, C are bounded positive integers satisfying (2).

**Added in proof*: Very recently the present authors have made a further extension to primes p, q with $2 \leq p$, $q < 30$.

The first step in our approach is to give a good upper bound for n whenever $|xy| > 1$. The best known estimates for linear forms in two logarithms enable one to derive, for every integer solution (x, y, n) with $|xy| > 1$, an explicit upper bound for n in terms of A, B and C; see Proposition A in Section 2. This bound is still, however, very large. One of the novelties of our approach is that, for concrete values of A, B and C, we are able to considerably improve the estimate so obtained by means of local arguments, provided that

$$\pm A \neq C \quad \text{and} \quad A \neq C,\ B \neq C. \tag{3}$$

This condition excludes the solutions (x, y, n) with $|xy| \leq 1$ when n cannot be bounded. To illustrate our improvement, we prove the following theorem. For applications, it suffices to consider the case when n is prime.

Theorem 1. *Suppose that* (2) *and* (3) *hold. For the pairs* (M_1, n_1), (M_2, n_2) *given in Table 1, and for every integer solution* (x, y, n) *of (1) with* $n \geq 3$ *prime, we have*

(i) $n \leq n_1$ *if* $\max\{A, B, C\} \leq M_1$

and

(ii) $n \leq n_2$ *if* $C = 1$ *and* $\max\{A, B\} \leq M_2$.

M_1	n_1	M_2	n_2
100	71	200	79
35	43	100	53
20	37	50	31
10	19	20	19

Table 1

It is worth comparing the pairs (M_1, n_1), (M_2, n_2) occurring in our table with those which are obtainable from Proposition A. We note that following the method of proof, Table 1 can be extended to larger values of M_1 and M_2 as well.

Our Theorem 1 together with the results and methods mentioned above enable us to completely resolve (1) for small positive values of A, B, C. To make the modular approach even more powerful, we shall use simultaneously the results of [15] and [7] on ternary equations of signature (n, n, n) and $(n, n, 3)$, respectively (cf. Proposition B).

Theorem 2. *Under the assumptions* (2) *and* $\max\{A, B, C\} \leq 10$, *all the integer solutions* (x, y, n) *to equation* (1) *with* $n \geq 3$, $|xy| > 1$ *and with*

$$B \pm A \neq C \quad \text{if} \quad C \geq 2 \tag{4}$$

are given by

(A,B,C)	*solutions* $(x,y),n$	(A,B,C)	*solutions* $(x,y),n$
$(1,2,6)$	$\pm(2,1),3$	$(3,7,3)$	$\pm(4,3),3$
$(1,2,8)$	$\pm(2,2),3$	$(3,10,1)$	$\pm(3,2),3$
$(1,2,10)$	$\pm(2,-1),\ \pm(4,3),3$	$(3,10,8)$	$\pm(6,4),3$
$(1,3,3)$	$\pm(3,2),3$	$(4,5,8)$	$\pm(2,2),3$
$(1,3,5)$	$\pm(2,1),3$	$(5,6,8)$	$\pm(2,2),3$
$(1,3,10)$	$\pm(13,9),3$	$(6,7,8)$	$\pm(2,2),3$
$(1,4,4)$	$\pm(2,1),3$	$(7,8,8)$	$\pm(2,2),3$
$(1,5,3)$	$\pm(2,1),3$	$(8,9,8)$	$\pm(2,2),3$
$(1,5,10)$	$\pm(5,3),3$	$(1,5,1)$	$(\pm3,\pm2),4$
$(1,6,2)$	$\pm(2,1),3$	$(1,6,10)$	$(\pm2,\pm1),4$
$(1,7,1)$	$\pm(2,1),3$	$(1,7,9)$	$(\pm2,\pm1),4$
$(1,9,1)$	$\pm(2,1),3$	$(1,8,8)$	$(\pm2,\pm1),4$
$(1,10,2)$	$\pm(2,1),3$	$(1,9,7)$	$(\pm2,\pm1),4$
$(2,5,2)$	$\pm(19,14),3$	$(1,10,6)$	$(\pm2,\pm1),4$
$(2,7,2)$	$\pm(3,2),3$		

If equation (1) has a solution with $x,y\in\{0,\pm1\}$, then our local approach does not work. The conditions (3) and (4) are required to exclude these trivial solutions. It is likely that apart from the trivial solutions, Theorem 1 and 2 are still valid without assuming (3) and (4). However, such a refinement cannot be achieved in general by the present methods.

For $C=1$, we are able to remove (3) and (4) and prove the following.

Theorem 3. *Under the assumptions* (2) *and* $\max\{A,B\}\le 20$*, all the solutions to equation*

$$|Ax^n-By^n|=1 \tag{5}$$

in integers $n\ge 3$*,* x,y *with* $|xy|>1$ *are given by*

(A,B)	*solutions* $(x,y),n$	(A,B)	*solutions* $(x,y),n$
$(1,7)$	$\pm(2,1),3$	$(5,13)$	$\pm(11,8),3$
$(1,9)$	$\pm(2,1),3$	$(5,17)$	$\pm(3,2),3$
$(1,17)$	$\pm(18,7),3$	$(8,17)$	$\pm(9,7),3$
$(1,19)$	$\pm(8,3),3$	$(8,19)$	$\pm(4,3),3$
$(1,20)$	$\pm(19,7),3$	$(11,19)$	$\pm(6,5),3$
$(2,15)$	$\pm(2,1),3$	$(1,5)$	$(\pm3,\pm2),4$
$(2,17)$	$\pm(2,1),3$	$(1,15)$	$(\pm2,\pm1),4$
$(3,10)$	$\pm(3,2),3$	$(1,17)$	$(\pm2,\pm1),4$

In the special case $A = 1$ we have the following.

Theorem 4. *If $B \leq 70$, all the solutions of equation*

$$|x^n - By^n| = 1 \tag{6}$$

in integers $n \geq 3$, x, y with $|xy| > 1$ are given by $(B, n, x, y) = (7, 3, \pm(2, 1))$, $(9, 3, \pm(2, 1))$, $(17, 3, \pm(18, 7))$, $(19, 3, \pm(8, 3))$, $(20, 3, \pm(19, 7))$, $(26, 3, \pm(3, 1))$, $(63, 3, \pm(4, 1))$, $(15, 4, \pm 2, \pm 1)$, $(17, 4, \pm 2, \pm 1)$, $(39, 4, \pm 5, \pm 2)$ and $(31, 5, \pm(2, 1))$.

It is interesting to observe that under the assumptions of Theorems 3 and 4 equations (5) and (6) have no solution with $|xy| > 1$ and $n > 5$.

We note that the techniques of our paper may also be extended with suitable perseverance to solve the corresponding equations in Theorems 2, 3 and 4 for larger values of A, B and C. Such extensions will be carried out in Part II of our paper.

As is known, binomial Thue equations can be applied to superelliptic equations. For example, under certain assumptions made on the integer $D > 0$, the results of [9], [21], [3] and [6] mentioned above enable one to determine the solutions of the equation

$$x(x + 1) = Dy^n \text{ in positive integers } x, y, n \text{ with } n \geq 3. \tag{7}$$

In [6], all solutions are listed when D is divisible by at most two primes which do not exceed 13. An immediate consequence of our Theorems 3 and 4 is as follows.

Corollary. *If x is a positive integer such that equation (7) has a solution in positive integers y, n and D with $n \geq 3$ and $D \leq 45$, then*

$$x \in \{1, 2, 3, 4, 5, 6, 7, 8, 15, 16, 26, 31, 80, 512, 624, 5831, 6859\}.$$

2. Auxiliary results

To prove our theorems we need some auxiliary results.

Set $M = \max\{A, B, 3\}$ and $\lambda = \log\left(1 + \frac{\log M}{|\log(A/B)|}\right)$.

Proposition A. *Suppose that (x, y, n) is an integer solution to (1) with $x > |y| > 0, n \geq 3$ and*

$$3\log(1.5|C/B|) \leq 7400\frac{\log M}{\lambda}, \frac{\log 2C}{\log 2} \leq 8\log M.$$

Then we have

$$n \leq \min\left(7400\frac{\log M}{\lambda}, 3106\log M\right).$$

PROOF. A similar result was proved by MIGNOTTE [17] with a weaker upper bound for n. Mignotte's estimate has been improved in [20] by iterated application of Baker's theory of logarithmic forms. □

The following Proposition B summarizes some recent results obtained by KRAUS [15], and BENNETT, VATSAL and YAZDANI [7] on ternary equations of the form

$$Ax^n + By^n = Cz^m \quad \text{with} \quad m \in \{3, n\}, \tag{8}$$

where A, B, C are given nonzero integers, $n \geq 3$, and x, y, z are unknown integers. Approaches to solving such equations, analogous to that employed by WILES [27] to prove Fermat's Last Theorem, are based on the connection between the putative integer solutions (x, y, z) of ternary equations, Frey curves and certain modular forms. In this direction significant contributions were also made among others by Frey, Serre, Darmon, Merel, Ribet, Bennett and Skinner.

For a given prime q and nonzero integer u, set

$$\mathrm{Rad}_q(u) = \prod_{p|u,\ p\neq q} p,$$

where the product is taken over primes p, and write $\mathrm{ord}_q(u)$ for the largest non-negative integer k with $q^k|u$. Suppose that for given A, B, C and $n \geq 3$, we have a solution (x, y, z) to (8) in nonzero integers.

- If $m = 3$ (see [7]) we assume, without loss of generality, that $3 \nmid Ax$ and $By^n \not\equiv 2 \pmod 3$. Further, suppose that C is cube free, A and B are nth-power free and that equation (8) does not correspond to one of the identities

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3 \quad \text{or} \quad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3.$$

We consider the elliptic curve

$$E : Y^2 + 3CXY + By^nY = X^3,$$

and set

$$N_n(E) = Rad_3(AB)\, Rad_3(C)^2 \varepsilon_3,$$

where

$$\varepsilon_3 = \begin{cases} 3^2, & \text{if } 9 \mid (2 + C^2By^n - 3Cz), \\ 3^3, & \text{if } 3 \,||\, (2 + C^2By^n - 3Cz), \\ 3^4, & \text{if } \mathrm{ord}_3(By^n) = 1, \\ 3^3, & \text{if } \mathrm{ord}_3(By^n) = 2, \\ 1, & \text{if } \mathrm{ord}_3(B) = 3, \\ 3, & \text{if } \mathrm{ord}_3(By^n) > 3 \text{ and } \mathrm{ord}_3(B) \neq 3, \\ 3^5, & \text{if } 3 \mid C. \end{cases}$$

• If $m = n$ (see [15]), then we may assume without loss of generality, that $Ax^n \equiv -1 \pmod 4$ and $By^n \equiv 0 \pmod 2$. The corresponding Frey curve is

$$E : Y^2 = X(X - Ax^n)(x + By^n),$$

and put

$$N_n(E) = Rad_2(ABC)\,\varepsilon_n,$$

where

$$\varepsilon_n = \begin{cases} 1, & \text{if} \quad \mathrm{ord}_2(ABC) = 4, \\ 2, & \text{if} \quad \mathrm{ord}_2(ABC) = 0 \text{ or } \mathrm{ord}_2(ABC) \geq 5, \\ 2, & \text{if} \quad 1 \leq \mathrm{ord}_2(ABC) \leq 3 \text{ and } xyz \text{ even}, \\ 8, & \text{if} \quad \mathrm{ord}_2(ABC) = 2 \text{ or } 3 \text{ and } xyz \text{ odd}, \\ 32, & \text{if} \quad \mathrm{ord}_2(ABC) = 1 \text{ and } xyz \text{ odd}. \end{cases}$$

We note that both for $m = 3$ and for $m = n$, the numbers $N_n(E)$ are closely related to the conductors of the above curves (cf. [7] and [15]).

Proposition B. *Suppose that A, B, C, x, y and z are nonzero integers with Ax, By and Cz pairwise coprime, $xy \neq \pm 1$, satisfying equation (8) with prime $n \geq 5$ and $n \nmid ABC$. Then there exists a cuspidal newform $f = \sum_{r=1}^{\infty} c_r q^r$ ($q := e^{2\pi iz}$) of weight 2, trivial Nebentypus character and level $N_n(E)$ for $N_n(E)$ given as above. Moreover, if we write K_f for the field of definition of the Fourier coefficients c_r of this form and suppose that p is a prime, coprime to $nN_n(E)$, then*

$$\mathrm{Norm}_{K_f/\mathbb{Q}}(c_p - a_p) \equiv 0 \pmod n,$$

where $a_p = \pm(p+1)$ (if $p \mid xy$) or $a_p \in S_{p,m}$ (if $p \nmid xy$), with

$$S_{p,3} = \{u : |u| < 2\sqrt{p}, \quad u \equiv p + 1 \pmod 3\}$$

and

$$S_{p,n} = \{u : |u| < 2\sqrt{p}, \quad u \equiv p + 1 \pmod 4\}.$$

Proof. This is a combination of some deep results of [7] and [15]. (For a survey on this topic, see also [4]). □

Remark. In the proof of Theorem 4, Proposition B will be applied simultaneously to certain equations both with signature $(n, n, 3)$ and with signature (n, n, n).

Proposition C. *If A, B and n are nonzero integers and $n \geq 3$, then, for $C = 1$, equation (5) has at most one solution in positive integers x, y.*

PROOF. See [2, Theorem 1.1]. We shall use this Proposition in the special case $B = A + 1$. Then $x = y = 1$ is a solution to (5), hence no further solution exists. □

We recall that for a finite set of primes S, an integer u is an S-unit if all its prime factors lie in S. The following profound result is due to BENNETT, GYŐRY, MIGNOTTE and PINTÉR [6].

Proposition D. *Let $S = \{p, q\}$ for p and q primes with $2 \le p,\ q \le 13$. If A, B, x, y, n are positive integers with A, B S-units and $n \ge 3$, then the only solutions to equation* (5) *are those with*

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

and

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

PROOF. This is Theorem 1.1 in [6]. □

We now consider equation

$$x^n + y^n = B\, z^n, \tag{9}$$

where $n > 3$ is a prime, B is a nonzero rational integer and x, y, z are coprime nonzero rational integers. Let $\phi(B)$ denote Euler's function.

Proposition E. *Suppose that n is coprime to $B\phi(B)$, $B^{n-1} \not\equiv 2^{n-1} \pmod{n^2}$ and* (9) *has a solution in pairwise relatively prime nonzero integers x, y and z. Then either* (i) *$n|z$ or (ii) $n|xy$, Bz is odd and $r^{n-1} \equiv 1 \pmod{n^2}$ for each divisor r of B.*

PROOF. Proposition E was proved in [5] (see also [10]). □

Assume that in (9) $n|B$, but $n \nmid z$. Let $n, p_1, \dots, p_r$ denote the distinct prime factors of B. For $r \ge 1$, denote by $f_1, \dots, f_r$ the smallest positive integers for which

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

and set $\mathrm{ord}_n(B) = N$.

Remark. If $N = 1$, then (9) has no solution x, y, z with $n \nmid z$. Indeed, in the opposite case (9) implies $n|x + y$ whence $n|\frac{x^n + y^n}{x+y}$, a contradiction.

In our equation (6), neither the modular approach nor the local arguments work when $n|B$. In this case we shall need the following two propositions whose proofs involved classical algebraic numbertheoretical methods. The next assertion is due to Maillet [16].

Proposition F. *Suppose that the prime n is regular. If $N \geq 1$, $N \equiv 0$ or $1 \pmod{n}$ and, for $r \geq 1$,*

$$\sum_{i=1}^{r} \frac{1}{f_i} \leq \frac{n-3}{n-1}, \tag{10}$$

then (9) has no solution in coprime nonzero rational integers x, y, z not divisible by n.

Let $\zeta = e^{2\pi i/n}$. Denote by h_0 the class number of the number field $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$, and by B_m the m-th Bernoulli number. We recall that $B_{2m+1} = 0$ for $m \geq 1$. The following result was proved in [6].

Proposition G. *Suppose that $N = 1$ or $N \geq 4$, 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 $r \geq 1$, then $\sum_{i=1}^{r} \frac{1}{f_i} \leq \frac{n-3}{2(n-1)}$ and $\frac{n-1}{f_i}$ is odd for $i = 1, \ldots, r$.*

Then (9) has no solution in coprime nonzero rational integers x, y, z which are not divisible by n.

As was mentioned in [6], the conditions (i) and (ii) are satisfied for all primes $n < 350$.

Lemma H. *If p and $q > 0$ are rational integers, then we have*

$$\left| \left(\frac{8}{7}\right)^{1/19} - \frac{p}{q} \right| > \frac{1}{5.85 \cdot 10^{45}\, q^{11.85}},$$

$$\left| \left(\frac{9}{7}\right)^{1/19} - \frac{p}{q} \right| > \frac{1}{6.22 \cdot 10^{45}\, q^{15.37}},$$

and

$$\left| \left(\frac{9}{8}\right)^{1/19} - \frac{p}{q} \right| > \frac{1}{6.64 \cdot 10^{45}\, q^{11.54}}.$$

Proof. These are special cases of a deep result of Bennett [2, Theorem 7.1]. □

3. Proofs of theorems

PROOF OF THEOREM 1. We show that if (2) and (3) hold then, for the pairs (M_1, n_1), (M_2, n_2) occurring in Table 1, equation (1) has no solution with $n > n_1$ if $\max\{A, B, C\} \leq M_1$, and with $n > n_2$ if $C = 1$ and $\max\{A, B\} \leq M_2$. Suppose, on the contrary, that such solutions (x, y, n) exist. Then in view of (3), $|xy| > 1$ must hold for each of these putative solutions. Further, in our case Proposition A applies and gives an upper bound $n_0(A, B, C)$ for n. Thus, for fixed A, B, C, it suffices to deal in (1) with the prime exponents n with $n_1 < n < n_0(A, B, C)$. To prove our theorem, we used a short MAGMA program which is based on the following version of the local method. For each 4-tuple (A, B, C, n) we search for a local obstruction by considering (1) modulo a prime of the form $p = 2kn + 1$, coprime to A, B and C, with $k \in \mathbb{N}$. For such a prime, there are at most $(2k+1)^2$ possible residue classes for $Ax^n - By^n$. If none of these contains C, then equation (1) is impossible modulo p. If we do not find such a prime with $k \leq 150$, then we test the solvability of the equation modulo n^2. Our MAGMA program proves that under the assumptions of Theorem 1 the assertions (i) and (ii) hold, except for the case $M_1 = 10$ and $(A, B, C, n) = (1, 2, 8, 31), (1, 8, 2, 31), (1, 8, 6, 31)$. However the corresponding equations are impossible modulo 4.

We remark that the number of triples (A, B, C) and the number of pairs (A, B) under consideration were 293651 and 11834, respectively. We checked the solvability of (1) for every triple (A, B, C) and for all primes n with $n_1 < n < n_0(A, B, C)$. The total CPU time required was about 10 days on a 3.0MHz personal computer. □

To prove our Theorems 2 to 4, it will be enough to solve the corresponding equations for $n = 4$ and for odd primes n. As will be seen from the values of the solutions x, y so obtained, no solutions exist for other values of $n \geq 3$.

PROOF OF THEOREM 4. For $B = 30, 42, 66$ and 70, our equation (6) was solved in [5] and [20]. In view of Proposition D, it suffices to deal with the cases when B is different from the above values, and has at least three distinct prime factors or the greatest prime factor of B is greater than 13; for the remaining values of B, see Table 2.

Proposition A gives the upper bound $n < 3106 \log B$ for each B under consideration. Using PARI we resolved the corresponding Thue equations (6) for $n = 3, 4, 5, 7, 11, 13$. We note that this subroutine of PARI is based on theoretical work of HANROT [13], and it works without assuming the GRH if the right-hand side of the Thue equation is 1 or if the conditional class group is trivial.

In the sequel we may suppose that $n \geq 17$. We have to solve equation (6) for the remaining values of B and for the primes n with $17 \leq n \leq 3106 \log B$.

Case 1) $n \nmid B$

We consider equation (6) as a ternary equation of the form (8) with $C = \pm 1$ and with signature $(n, n, 3)$ or (n, n, n), according as B is odd or even. By Proposition B there must exist, for each B in question, modular forms with the properties specified there.

In our proofs we need a great number of data concerning modular forms. To compute the necessary data, we used the subroutine of MAGMA, developed by Stein [24]. For the values of B under consideration, the possible levels of the corresponding modular forms and the CPU time for calculating the basic arithmetical data of forms (dimension, Fourier coefficients c_2, c_3, c_5, c_7 and c_{11}) on a 3.0MHz PC, see Table 2.

B	signature	levels	CPU time (sec)
$p, 17 \leq p \leq 67$ prime	$(n, n, 3)$	$3p, 9p, 27p$	2019
$2p, p = 17, 19, 23, 29, 31$	(n, n, n)	$2p, 32p$	702
$3p, p = 17, 19, 23$	$(n, n, 3)$	$3p, 81p$	96
$4p, p = 17$	(n, n, n)	$2p, 8p$	48

Table 2

We recall that K_f denotes the field generated by the Fourier coefficients of a modular form f. For every modular form f under consideration, set

$$A_{2,3} = \mathrm{Norm}_{K_f/\mathbb{Q}}(c_2 - 3)\,\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2 + 3),$$

and

$$A_{p,m} = \mathrm{Norm}_{K_f/\mathbb{Q}}(c_p - (p+1))\,\mathrm{Norm}_{K_f/\mathbb{Q}}(c_p + (p+1)) \prod_{i \in S_{p,m}} \mathrm{Norm}_{K_f/\mathbb{Q}}(c_p - i),$$

where $m \in \{3, n\}, p$ is a prime, coprime to n and the level, and $S_{p,m}$ is the set defined in Proposition B.

For the values B and n in question, we resolved our equation (6) by the way presented below. To illustrate our method we give detailed examples both in the odd and in the even cases.

Set $B = 53$. In the *odd* case, xy is even. Then, by Proposition B, there exists at least one modular form f of level N contained in $\{3 \cdot 53, 9 \cdot 53, 27 \cdot 53\}$ such that

$$n \mid \gcd(A_{2,3}, A_{5,3}, A_{7,3}, A_{11,3}). \tag{11}$$

We may assume that f is not a rational modular form (so that K_f is a proper extension of $\mathbb{Q}$), since otherwise the Hasse–Weil bound (see e.g. [23]) gives $n \leq 2\sqrt{2}+3$, which is a contradiction. There are 17 non-rational modular forms with levels under consideration, and checking (11) for each of these modular forms we infer that $n \leq 13$. But this contradicts the assumption that $n \geq 17$. The same argument applies to each pair (B, n) with B odd, except for the pairs occurring in Table 3 for which (11) holds.

B	Levels	n
37	$111, 333, 999$	19
47	$141, 423, 1269$	23
59	$177, 531, 1593$	$19, 29$
61	$183, 549, 1647$	31
67	$201, 603, 1809$	17
71	$213, 639, 1917$	31

Table 3

Apart from the pairs $(B, n) = (47, 23)$ and $(59, 29)$, we apply to the other pairs Propositions E and F to prove that the corresponding Thue equations of the form (6) have no solution (x, y) with $|xy| > 1$. For example, if $(B, n) = (61, 31)$, it is easy to check that $(31, 60 \cdot 61) = 1, 61^{30} \not\equiv 2^{30}\ (31^2)$ and $61^{30} \not\equiv 1\ (31^2)$, thus Proposition E gives that 31 must divide y. Then we can rewrite the equation $x^{31} - 61y^{31} = 1$ as $x^{31} - 61 \cdot 31^N \cdot y_1^{31} = 1$, where $31|N$ and $31 \nmid y_1$. With the notation of Proposition F we have $r = 1, f_1 = 2$ and since $1/2 < 14/15$, Proposition F yields a contradiction.

Consider again the remaining equations $x^{23} - 47y^{23} = \pm 1$ and $x^{29} - 59y^{29} = \pm 1$ as ternary equations. Proposition B with signature $(n, n, 3)$ did not make it possible to solve these equations. We now apply Proposition B with signature (n, n, n). Then the levels of the corresponding modular forms are 94 and 118, respectively. If (x, y) is a solution of the first, resp. second equation, then one can show by local arguments that $139|xy$, resp. $233|xy$. In the case $|xy| > 1$ Proposition B implies that

$$23| \operatorname{Norm}_{K_f/\mathbb{Q}}(c_{139} - 140)) \cdot \operatorname{Norm}_{K_f/\mathbb{Q}}(c_{139} + 140)$$

and

$$29| \operatorname{Norm}_{K_f/\mathbb{Q}}(c_{233} - 234) \cdot \operatorname{Norm}_{K_f/\mathbb{Q}}(c_{233} + 234)$$

for some modular form f of level 94, resp. 118. However, an easy calculation shows that these relations are impossible for every modular form under consideration.

The situation is more difficult in the *even* case. Take for example $B = 46$. We recall that then $n \leq 11892$. It follows from Proposition B with signature (n, n, n) that if there exists an associated modular form then its level is $23 \cdot 2$ or $23 \cdot 32$. There are one rational and 8 non-rational modular forms having these levels. For the non-rational modular forms Proposition B implies as above the relation

$$n | \gcd(A_{3,n}, A_{5,n}, A_{7,n}).$$

It is easy to check that this yields $n \leq 13$, which is excluded by assumption.

The level of the rational modular form in question is $23 \cdot 2$. In this rational case $A_{p,n} = 0$ for small primes p, so we have to apply another argument. For every exponent $n \leq 11892$ one can calculate a prime $p_1 = p_1(n)$ with the property $p_1 \equiv 1$ modulo n such that $p_1 | xy$. Then Proposition B implies that

$$n | \operatorname{Norm}_{K_f/\mathbb{Q}}(c_{p_1} - (p_1 + 1)) \cdot \operatorname{Norm}_{K_f/\mathbb{Q}}(c_{p_1} + (p_1 + 1)). \tag{12}$$

If this does not hold, then (6) has no solution for this n and $B = 46$. If (12) holds then we calculate a new prime $p_2 = p_2(n)$ with $p_2 \equiv 1$ modulo n and $p_2 | xy$, and we continue this procedure. The exponents n for which we have to calculate one more localization prime p_2 are listed in Table 4. For these second primes p_2 the relation corresponding to (12) does not hold, which proves our theorem for $B = 46$.

n	p_1	p_2
79	317	1423
233	467	1399
1231	19697	22159
2243	71777	80749
3301	52817	61223
4733	9467	123059
6359	50873	152617
8123	113723	211199
9341	74729	242867

Table 4. $N = 2 \cdot 23$

Summarizing the above approach (which is developed in [20] for some scattered cases), we have a rather effective sieve for the exponent n, apart from the case when B is even and the corresponding modular forms are rational. As was seen above, this case needs a relatively long, but straightforward calculation. Table 5 shows the values of these B, the maximum of the (first or, if necessary,

second) localization primes p, the corresponding levels with the numbers of rational modular forms, and the required CPU time on a 3.0MHz PC.

B	maximum of p	levels	CPU time (hour)
34	496747	$34(1), 544(6)$	3.65
38	496747	$38(2), 608(6)$	4.01
46	496747	$46(1), 736(0)$	0.44
58	780583	$58(1), 928(2)$	2.37
60	496747	$30(1), 120(2)$	1.42
62	729661	$62(1), 992(0)$	1.00
68	542599	$34(1), 136(2)$	1.71

Table 5

Case 2) $n|B$

In this case $n \geq 17$ and $B \leq 70$ imply that $n||B$ and $n \leq 67$. If now $B = n$, it follows from Proposition G that equation (6) has no solution with $|xy| > 1$. Suppose that n is a proper divisor of B. Since $n = 37$ is the smallest irregular prime and $2 \cdot 37 > 70$, n must be regular. It is easy to check that the condition (10) of Proposition F holds for each pair (B, n) under consideration. Thus Proposition F proves that for these pairs (B, n) no solution exists with $|xy| > 1$, which completes the proof of our theorem. □

Proof of Theorem 3. In view of Theorem 4 we may assume that $A > 1$. If $B - A = 1$ then $x = y = 1$ is a solution of (5), and Proposition C gives that equation (5) has no solution with $|xy| > 1$. For $n \leq 7$, we resolved (5) by means of PARI. Hence we may assume that $B - A > 1$ and $n \geq 11$. Then Theorem 1 yields $n \leq 19$.

Using first Proposition D and then applying the local method, we solved all the equations under consideration with 9 exceptions. For the remaining 9 triples (A, B, n) which are listed in Table 6 below we resolved equations (5) by PARI.

(A, B, n)	CPU-time (min)	(A, B, n)	CPU-time (min)
$(3, 14, 13)$	1	$(5, 18, 13)$	3
$(3, 19, 11)$	1	$(6, 17, 13)$	3
$(4, 19, 13)$	1	$(10, 13, 13)$	3
$(5, 14, 13)$	2	$(17, 19, 13)$	48
$(5, 17, 11)$	1		

Table 6

□

PROOF OF THEOREM 2. Let (A, B, C, x, y, n) be a fixed solution to equation (1) with $\max\{A, B, C\} \le 10$ which satisfies conditions (2) and (4). By Theorem 3 it suffices to consider the case when $C > 1$. If $n = 3$, 4, 5, 7 then we can solve again the corresponding Thue equations by MAGMA for each possible value of A, B and C, and we obtain the solutions listed in Theorem 2. In the sequel we assume that $n \ge 11$ is a prime and $C > 1$.

1) First assume that $(A - C)(B - C) \neq 0$.

In this case, Theorem 1 yields $n \le 19$. Using the local method presented in the proof of Theorem 1, we showed that for most of the 4-tuples (A, B, C, n) the corresponding equation (1) has no solution. The local method does not work for the following exceptional 4-tuples:

$(A, B, C, n) \in \{(1, 2, 10, 17), (1, 4, 7, 19), (1, 8, 10, 17), (1, 8, 10, 19), (1, 10, 2, 17), (1, 10, 8, 19), (2, 3, 7, 13), (2, 3, 9, 13), (2, 5, 10, 19), (3, 4, 8, 19), (3, 4, 10, 19), (3, 5, 9, 17), (3, 5, 9, 19), (3, 10, 4, 19), (5, 6, 9, 17), (5, 9, 3, 19), (7, 8, 9, 19), (7, 9, 3, 13), (7, 9, 8, 19), (8, 9, 6, 11), (8, 9, 7, 19)\}$.

If $(A, B, C, n) \in \{(1, 8, 10, 17), (1, 8, 10, 19), (1, 10, 8, 19), (3, 4, 8, 19), (3, 4, 10, 19), (3, 10, 4, 19)\}$ or $(A, B, C, n) \in \{(2, 3, 9, 13), (3, 5, 9, 17), (3, 5, 9, 19), (5, 6, 9, 17), (5, 9, 3, 19), (8, 9, 6, 11)\}$ then the corresponding equations are impossible mod 2 or mod 3.

If $(A, B, C, n) = (1, 2, 10, 17)$, $(1, 10, 2, 17)$ or $(2, 5, 10, 19)$, then x or y is even. We consider these equations as ternary equations with signature (n, n, n). Then by Proposition B the level of the associated modular forms should be 10. However, there is no modular form of this level.

For $(A, B, C, n) = (1, 4, 7, 19)$, Proposition B shows that the level of the associated modular forms is 14 or 56. Further, one can see that $191 \mid xy$ for every solution x, y. In view of Proposition B it is enough to check the relation

$$19 \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(c_{191} - 192) \cdot \mathrm{Norm}_{K_f/\mathbb{Q}}(c_{191} + 192), \tag{13}$$

for every modular form f of level 14 and 56, where c_{191} is the 191st Fourier coefficient of f. There are one modular form of level 14 and two modular forms of level 56, and the corresponding coefficients are $c_{191} = 24$ and $c_{191} = -8, -16$, respectively. Thus condition (13) does not hold.

If $(A, B, C, n) = (2, 3, 7, 13)$ and (x, y) is a solution of the equation $2x^{13} - 3y^{13} = 7$, then it is easy to verify that $53 \cdot 443 \mid xy$. Proposition B implies that there is at least one modular form f of level $2 \cdot 21 = 42$ or $32 \cdot 21 = 672$ with

$$13 \mid \gcd(\mathrm{Norm}_{K_f/\mathbb{Q}}(c_{53} - 54)\ \mathrm{Norm}_{K_f/\mathbb{Q}}(c_{53} + 54), \\ \mathrm{Norm}_{K_f/\mathbb{Q}}(c_{443} - 444)\ \mathrm{Norm}_{K_f/\mathbb{Q}}(c_{443} + 444)).$$

There are one, resp. ten modular forms of level 42, resp. 672. An easy MAGMA program gives that the previous relation does not hold for any modular form of these levels.

Finally, for the remaining cases $(A,B,C,n) = (7,8,9,19)$, $(7,9,8,19)$ or $(8,9,7,19)$, one can apply Lemma H to show that equation (1) has no solutions. For example, if $(A,B,C,n) = (7,8,9,19)$, then (1) implies

$$(8/7)^{18/19} \left| \prod_{i=1}^{18} \sin i\frac{2\pi}{19} \right| \left| (8/7)^{1/19} - x/y \right| \leq \frac{9}{7y^{19}}.$$

The constant on the left-hand side is 1/12157.56..., thus we obtain by the first relation of Lemma H that $y < 9.72 \cdot 10^6$. Then we used an algorithm developed by Pethő [19] for finding the small solutions of Thue equations to resolve the corresponding equation. This completes the first part of the proof.

2) Next consider the case when $(A-C)(B-C) = 0$.

In this case equation (1) leads to an equation of the form

$$|x_1^n - B_1 y_1^n| = 1 \text{ in integers } x_1, y_1, \tag{14}$$

where B_1 is a positive integer not having prime factor greater than 7. Apart from the cases when in (1)

$$(A,B) \in \{(3,10),(5,6),(6,7),(7,10)\}, \tag{15}$$

in the new equation (14) B_1 has at most two distinct prime factors. But then Proposition D applies and gives the possible solutions.

In the remaining cases listed in (15) we infer that

$$B_1 \in \{10 \cdot 3^{n-1}, 3 \cdot 10^{n-1}, 6 \cdot 5^{n-1}, 5 \cdot 6^{n-1}, 7 \cdot 6^{n-1}, 6 \cdot 7^{n-1}, 10 \cdot 7^{n-1}, 7 \cdot 10^{n-1}\}.$$

In each case we get an explicit upper bound n_0 for n by means of Proposition A. We note that if $(A,B) = (5,6)$ or $(6,7)$, then Theorem 3 of [17] gives the even better bound $n_0 = 600$ for n. We resolved equation (14) for each of the B_1 under consideration with $11 \leq n \leq n_0$. We now illustrate our method on resolving (14) for $B_1 = 6 \cdot 5^{n-1}$, which equation comes from (1) with $(A,B) = (5,6)$, i.e. from the equation

$$|5x^n - 6y^n| = 5. \tag{16}$$

Applying Proposition B with signature (n,n,n) we infer that if x_1, y_1 is a solution to (14) with $|x_1 y_1| > 1$ then there is at least one modular form of level $N = 2 \cdot 15$

or $32 \cdot 15$. There are one modular form of level 30 and 8 modular forms of level 480. All these modular forms are one-dimensional. Since n is bounded, we can apply the same arguments as in the proof of our Theorem 4. Namely, for each modular form and for each n under consideration we calculate a prime $p_1 = p_1(n)$ with $p_1 | x_1 y_1$. Then Proposition B implies (12). If (12) does not hold, we are done. Otherwise we continue the procedure with a second localization prime $p_2 = p_2(n)$ with $p_2 | x_1 y_1$ and we arrive in each case at a contradiction with (12). The following Tables 7A and 7B contain those exponents n and primes p_1 for which we had to find a second prime p_2.

n	p_1	p_2
37	149	223
73	293	439
97	389	971
157	1571	3769
241	1447	2411
277	1109	1663
313	1879	5009
577	2309	3463

Table 7a. $N = 2 \cdot 15$

Form	n	p_1	p_2
f_1	59	709	827
f_2	43	173	431
f_3	59	709	827
f_4	139	557	1669
f_5	139	557	1669
f_6	67	269	1609
	127	509	2287
f_7	43	173	431
f_8	67	269	1609
	127	509	2287

Table 7b. $N = 32 \cdot 15$ □

Acknowledgements. The authors are grateful to Professors M. A. Bennett and A. Kraus for their helpful remarks.

References

[1] A. Baker, Contributions to the theory of diophantine equations, *Phil. Trans. Roy. Soc. London* **263** (1968), 173–208.

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

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

[4] M. A. Bennett, Recipes for ternary diophantine equations of signature (p, p, k), in: RIMS Kokyuroku, Vol. 1319, *RIMS, Kyoto University, Kyoto, Japan*, 2003, 51–55.

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

[6] M. A. Bennett, K. Győry, M. Mignotte and Á. Pintér, Binomial Thue equations and polynomial powers, *Compositio Math.* **142** (2006), 1103–1121.

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

[8] Y. Bugeaud, M. Mignotte and S. Siksek, A multi-Frey approach to some multi-parameter families of diophantine equations, *Canad. J. Math.* (*to appear*).

[9] H. Darmon and L. Merel, Winding quotient and some variants of Fermat's Last Theorem, *J. Reine Angew. Math.* **490** (1997), 81–100.

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

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

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

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

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

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

[16] E. Maillet, Sur les équations indéterminés de la forme $x^\lambda + y^\lambda = cz^\lambda$, *Acta Math.* **24** (1901), 247–256.

[17] M. Mignotte, A note on the equation $ax^n - by^n = c$, *Acta Arith.* **75** (1996), 287–295.

[18] L. J. Mordell, Diophantine Equations, *Academic Press*, *London – New York*, 1969.

[19] A. Pethő, On the resolution of Thue inequalities, *J. Symbolic Comput.* **4** (1987), 103–109.

[20] Á. Pintér, On the power values of power sums, *J. Number Theory* (*to appear*).

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

[22] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, *Cambridge University Press*, *Cambridge*, 1986.

[23] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer*, 1994.

[24] W. Stein, Modular forms database, Current web address http://modular.fas.harvard.edu/Tables.

[25] A. Thue, Über Annäherungenswerte algebraischer Zahlen, *J. Reine Angew. Math.* **135** (1909), 284–305.

[26] R. Tijdeman, Some applications of Baker's sharpened bounds to diophantine equations, Sém. Delange-Pisot-Poitou, 1974/75, Paris, Exp. 24, 7pp.

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

KÁLMÁN GYŐRY
MATHEMATICAL INSTITUTE
NUMBER THEORY RESEARCH GROUP OF THE HUNGARIAN ACADEMY OF SCIENCES
UNIVERSITY OF DEBRECEN
4010 DEBRECEN
HUNGARY

E-mail: gyory@math.klte.hu

ÁKOS PINTÉR
MATHEMATICAL INSTITUTE
NUMBER THEORY RESEARCH GROUP OF THE HUNGARIAN ACADEMY OF SCIENCES
UNIVERSITY OF DEBRECEN
4010 DEBRECEN
HUNGARY

E-mail: apinter@math.klte.hu

(Received December 16, 2005; revised October 13, 2006)