Bull. London Math. Soc. 36 (2004) 683–694
DOI: 10.1112/S0024609304003480

PRODUCTS OF CONSECUTIVE INTEGERS

MICHAEL A. BENNETT

Abstract

In this paper, a number of results are deduced on the arithmetic structure of products of integers in short intervals. By way of an example, work of Saradha and Hanrot, and of Saradha and Shorey, is completed by the provision of an answer to the question of when the product of k out of $k+1$ consecutive positive integers can be an 'almost' perfect power. The main new ingredient in these proofs is what might be termed a practical method for resolving high-degree binomial Thue equations of the form $ax^n - by^n = \pm 1$, based upon results from the theory of Galois representations and modular forms.

1. *Introduction*

A celebrated theorem of Erdős and Selfridge [**6**] states that the product of $k \geqslant 2$ consecutive integers can never be a perfect nth power, for $n \geqslant 2$. In the particular case $k = 2$, this amounts to the observation that there are no consecutive positive nth powers. If we shift this problem slightly, however, and ask to find two consecutive integers whose product is, say, twice an nth power, then it becomes a rather more formidable task. There are infinitely many such pairs for $n = 2$, corresponding to Pell equations of the form $u^2 - 2v^2 = \pm 1$. The only known proof that the only pair for larger values of n is $(1, 2)$ depends upon a modification of Wiles' proof of Fermat's last theorem (see [**5**]).

In this paper, we will investigate a rather innocent-looking Diophantine equation, closely related to these questions. Our main result is the following theorem.

Theorem 1.1. *If m, t, α, β, y and n are nonnegative integers with $n \geqslant 3$ and $y \geqslant 1$, then the only solutions to the equation*

$$m(m + 2^t) = 2^\alpha 3^\beta y^n$$

are those with

$$m \in \{2^t, 2^{t\pm1}, 3 \cdot 2^t, 2^{t\pm3}\}.$$

We will actually deduce Theorem 1.1 from a pair of results, the first of which constitutes the bulk of the work in this paper.

Theorem 1.2. *Suppose that $a < b$ are positive integers with $ab = 2^\alpha 3^\beta$ for α, β nonnegative integers. If $n \geqslant 3$ is an integer, then the only solutions in positive integers x and y to the Diophantine equation $ax^n - by^n = \pm 1$ are given by*

$$(a, b, x, y, n) = (1, 2, 1, 1, n), (2, 3, 1, 1, n), (3, 4, 1, 1, n), (8, 9, 1, 1, n), (1, 9, 2, 1, 3).$$

Received 12 November 2002; revised 22 October 2003.

2000 *Mathematics Subject Classification* 11D41, 11D61.

The author was supported in part by a grant from NSERC.

The second result that we require is part of recent joint work of Vatsal, Yazdani and the author.

Theorem 1.3 (Bennett, Vatsal, Yazdani [**4**]). *If α and β are nonnegative integers and $n \geqslant 5$ is prime, then the equation*

$$x^n + 3^\beta y^n = 2^\alpha z^3$$

has no solution in coprime nonzero integers (x, y, z) with $|xy| > 1$.

The proofs of the above theorems are, perhaps surprisingly, rather involved (or, I should say, this is the case for our proofs). Some of the ingredients include results on ternary Diophantine equations coming from the theory of Galois representations and modular forms, bounds for solutions of binomial Thue equations derived both from the method of Thue–Siegel and from lower bounds for linear forms in logarithms of algebraic numbers, and local methods. We wish to emphasize that the techniques that we employ are, at least in part, new, and have not been applied in such a setting before. Indeed, our main goal in writing this paper is to exhibit a concrete example of a polynomial-exponential equation where:

(i) traditional techniques based on lower bounds for linear forms in logarithms fail to provide a complete solution, and
(ii) the addition of arguments based upon Frey curves proves adequate to the task.

A couple of corollaries may be of interest. The first is a generalization of classical work of Størmer [**17**] and Ljunggren [**11**] on Diophantine equations of the form $x^2 - 2^\alpha y^n = \pm 1$ (which has rather curious applications to, for example, the computation of π; see [**13**] for details).

Corollary 1.4. *Let $D = 2^\alpha 3^\beta$, where α and β are nonnegative integers. Then the only solutions to the equation*

$$x^2 - Dy^n = \pm 1 \tag{1}$$

in positive integers (x, y, n) with $n \geqslant 3$ are given by

$$(x, y, n, D) = \begin{cases} (1,1,n,2), (2,1,n,3), (3,1,n,8), (5,1,n,24), \\ (7,1,n,48), (17,1,n,288), (3,2,3,1), (5,2,3,3), \\ (7,2,4,3), (17,2,5,9), (239,13,4,2). \end{cases}$$

Another straightforward corollary of Theorem 1.1 (and, indeed, a motivation for this paper) is an extension of a result of Hanrot, Saradha and Shorey [**8**]. Before we state this, we require a little background material. The theorem of Erdős and Selfridge [**6**], to which we alluded at the beginning of this introduction, states that the equation

$$m(m+1)\dots(m+k-1) = y^n$$

has no solutions in positive integers x, y, k and n, with $k \geqslant 2$ and $n \geqslant 2$. Many generalizations of this result, suggested in [**6**] or otherwise, have since been considered. For example, we may treat the Diophantine equation

$$(m+d_1)(m+d_2)\dots(m+d_t) = by^n, \tag{2}$$

where m, t, b, y and n are positive integers with $n \geqslant 3$, where $P(b)$, the greatest prime divisor of b, is 'small', and where the d_i are distinct integers from a short interval. Along these lines, assuming that

$$0 \leqslant d_1 < d_2 < \ldots < d_t < k, \quad m > k^n \quad \text{and} \quad P(b) \leqslant k,$$

Saradha [**15**] (for $k \geqslant 4$) and Győry [**7**] (for $k \in \{2, 3\}$) were able to show that equation (2) has no solutions, provided that $k = t$. In the case $k = t + 1$, a similar conclusion was obtained by Saradha [**15**] for $k \geqslant 9$, and by Hanrot, Saradha and Shorey [**8**] if $6 \leqslant k \leqslant 8$. Theorem 1.1 enables us to extend this result to $k \geqslant 3$ as follows.

Corollary 1.5. *Let $t \in \{2, 3, 4\}$. Then equation (2) has only the following solutions in positive integer m and integers $0 = d_1 < \ldots < d_t \leqslant t$, where $P(b) \leqslant t+1$ and $n \geqslant 2$ (or $n \geqslant 3$ if $t = 2$).*

t	m	d_i
2	$1, 2, 3, 8$	$\{0, 1\}$
2	$1, 2, 4, 6, 16$	$\{0, 2\}$
3	$1, 2, 48$	$\{0, 1, 2\}$
3	$1, 3, 24$	$\{0, 1, 3\}$
3	$1, 6$	$\{0, 2, 3\}$

t	m	d_i
4	$1, 2, 3$	$\{0, 1, 2, 3\}$
4	$1, 2, 4, 8$	$\{0, 1, 2, 4\}$
4	$1, 2, 5$	$\{0, 1, 3, 4\}$
4	$1, 2, 6$	$\{0, 2, 3, 4\}$

It does not seem that the techniques of [**8**] may be adapted to handle the cases considered here. Moreover, our approach does not require the restriction to $m > (t+1)^n$ (which is, admittedly, a mild one).

2. *Proof of Theorem* 1.1

Let us begin by proving Theorem 1.1, assuming that Theorem 1.2 holds. Suppose that we have

$$m(m + 2^t) = 2^\alpha 3^\beta y^n$$

for integers $n \geqslant 3$, $y \geqslant 1$ and $\alpha, \beta, t \geqslant 0$, where, without loss of generality, y is coprime to 6. Write

$$m = 2^{\alpha_0} 3^{\beta_0} m_1,$$

with m_1 also coprime to 6. We investigate the cases $\alpha_0 < t$, $\alpha_0 = t$ and $\alpha_0 > t$ separately.

If we have $\alpha_0 < t$, then $\alpha = 2\alpha_0$ and hence, if further $\beta_0 = 0$, from

$$m_1(m_1 + 2^{t-\alpha_0}) = 3^\beta y^n$$

there exist odd coprime positive integers a and b such that $m_1 = a^n$ and

$$m_1 + 2^{t-\alpha_0} = 3^\beta b^n,$$

whence

$$a^n - 3^\beta b^n = -2^{t-\alpha_0}. \tag{3}$$

By Theorem 1.3, if n has a prime factor exceeding 3, then $a = b = 1$, and so an old result of Levi ben Gerson (see [**13**]) implies that $\beta = 1$ and $t - \alpha_0 = 1$, or else $\beta = 3$ and $t - \alpha_0 = 3$. These conditions lead to $m = 2^{t-1}$ and $m = 2^{t-3}$, respectively. For the remaining values of n, without loss of generality, we may suppose that $n \in \{3, 4\}$.

If $n = 3$ and $\beta \equiv 1 \pmod 3$, we may appeal to a result of Selmer [**16**], to the effect that the ternary equations

$$X^3 + 3Y^3 = 2^\gamma Z^3 \qquad (\gamma \in \mathbb{Z})$$

have no solutions in coprime integers X, Y and Z with $|XYZ| > 1$. In our situation, this implies that $a = b = 1$, and so $t - \alpha_0 = 1$, whereby $m = 2^{t-1}$. If, on the other hand, $\beta \equiv 2 \pmod 3$, since the Diophantine equation $X^3 - 9Y^3 = 2^k$ has only the solutions $(X, Y) = (1, 0)$, $(X, Y) = (-2, -1)$ and $(X, Y) = (-1, -1)$ (this may be readily proved using standard techniques for Thue–Mahler equations; see, for example, [**18**] or [**19**]), we conclude that $m = 2^{t-3}$. Finally, if $\beta \equiv 0 \pmod 3$, we find, by parity, that $a^2 + ab + b^2 = 1$, contradicting the fact that $a, b \in \mathbb{N}$.

If $n = 4$, considering equation (3) modulo 3 and 16 and factoring the left-hand side of (3) leads to the conclusion that only the equations

$$a^4 - 3^\beta b^4 = -2, \quad \text{with } \beta \equiv 1 \pmod 4$$

and

$$a^4 - 3^\beta b^4 = -8, \quad \text{with } \beta \equiv 2 \pmod 4$$

have solutions in odd coprime positive integers. The second of these, after factoring, has just the solution $a = b = 1$, $\beta = 2$, again leading to $m = 2^{t-3}$. A like conclusion (that is, that $a = b = \beta = 1$ is the only positive solution) obtains for the first equation, from work of Ljunggren [**10**], and leads to $m = 2^{t-1}$.

Next, suppose that $\alpha_0 < t$ and $\beta_0 > 0$ (so that $\beta_0 = \beta$). We can thus find odd coprime positive integers a and b for which

$$m_1 = a^n \quad \text{and} \quad 3^{\beta_0} m_1 + 2^{t-\alpha_0} = b^n,$$

and so

$$b^n - 3^{\beta_0} a^n = 2^{t-\alpha_0}. \tag{4}$$

Again, if n has a prime factor $p \geqslant 5$, then Theorem 1.3 yields $a = b = 1$, contradicting equation (4), the two sides of which have opposite signs. If $n = 4$, local considerations (modulo 3 and 16) imply that (4) has no positive odd solutions. The case $n = 3$ of (4) may be handled as per equation (3), only this time with no corresponding solutions.

For the remaining possibilities, where $\alpha_0 \geqslant t$, we appeal to Theorem 1.2 (whose proof will follow this section). If $\alpha_0 = t$ and $\beta_0 = 0$, we find that

$$m_1(m_1 + 1) = 2^{\alpha - 2\alpha_0} 3^\beta y^n,$$

and so

$$a^n - 2^{\alpha - 2\alpha_0} 3^\beta b^n = -1$$

for some odd coprime $a, b \in \mathbb{N}$, whereby, from Theorem 1.2, $a = b = \alpha - 2\alpha_0 = 1$ and $\beta = 0$ (so that $m = 2^t$). If $\alpha_0 = t$ and $\beta_0 > 0$, then

$$m_1(3^{\beta_0} m_1 + 1) = 2^{\alpha - 2\alpha_0} y^n,$$

and so

$$3^{\beta_0} a^n - 2^{\alpha - 2\alpha_0} b^n = -1,$$

for $a, b \in \mathbb{N}$ odd, whence $a = b = 1$ and $\beta_0 = 1$ (so that $m = 3 \cdot 2^t$).

If $\alpha_0 > t$ and $\beta_0 = 0$, then $\alpha = \alpha_0 + t$ and

$$m_1(2^{\alpha_0 - t} m_1 + 1) = 3^\beta y^n,$$

so that

$$3^\beta a^n - 2^{\alpha_0 - t} b^n = 1.$$

Again applying Theorem 1.2 gives $a = b = 1$, and so $m \in \{2^{t+1}, 2^{t+3}\}$. Finally, if $\alpha_0 > t$ and $\beta_0 > 0$, then

$$m_1(3^{\beta_0} 2^{\alpha_0 - t} m_1 + 1) = y^n,$$

and so

$$a^n - 3^{\beta_0} 2^{\alpha_0 - t} b^n = 1,$$

which, by Theorem 1.2, has no positive integral solutions. This completes the proof of Theorem 1.1.

3. *Proof of Theorem* 1.2

We now turn our attention to proving Theorem 1.2. To do this, we will appeal to a pair of results on ternary Diophantine equations that follow from the theory of Galois representations and modular forms. The first of these combines work of Kraus [**9**], Darmon and Merel [**5**] and Ribet [**14**], and provides a generalization of the approach of Wiles for ternary equations of signature (n, n, n).

THEOREM 3.1. *If a and b are coprime positive integers with $ab = 2^\alpha 3^\beta$, where α and β are nonnegative integers such that $\alpha = 0$ or $\beta = 0$ or $\alpha \geqslant 4$, then, if $n \geqslant 5$ is prime, the equation*

$$ax^n + by^n = z^n$$

has no solution in coprime nonzero integers (x, y, z) with $|xy| > 1$.

Generalizing some work of Darmon and Merel [**5**], Vatsal, Yazdani and the author have proved analogous results for ternary equations of signature $(n, n, 3)$. As easy consequence of these methods is the following lemma.

LEMMA 3.2. *If a and b are coprime positive integers with $ab = 2^\alpha 3^\beta$, where α and β are positive integers with $\beta > 1$, then, if $n \geqslant 5$ is prime, the equation*

$$ax^n + by^n = z^3$$

has no solution in coprime nonzero integers (x, y, z) with $|xy| > 1$.

Proof. To prove the above result, we argue as in [**4**]. The fact that there exist no weight 2 cuspidal newforms with trivial Nebentypus character and level $N \in \{2, 6, 18\}$, leads, via [**4**, Lemma 3.4], to the conclusion stated here. $\square$

Finally, through an application of the hypergeometric method of Thue and Siegel, the author has proved the next theorem.

THEOREM 3.3 (Bennett [**2**]). *If a, b and n are integers with $ab \neq 0$ and $n \geqslant 3$, then the equation*

$$|ax^n - by^n| = 1 \tag{5}$$

has at most one solution in positive integers (x, y).

Applying these results (with $z = \pm 1$), it remains, for $n \geqslant 5$ prime, to solve equation (5) with (a, b) equal to $(1, 6)$, $(1, 12)$, $(1, 24)$ and $(3, 8)$. To deal with these equations, we use a lower bound for linear forms in logarithms of algebraic numbers: say, that implicit in the following result of Mignotte.

THEOREM 3.4 (Mignotte [**12**]). *Let*

$$F(x, y) = ax^n - by^n, \qquad a \neq b,$$

be a binary form of degree $n \geqslant 3$, with positive integer coefficients a and b. Put $A = \max\{a, b, 3\}$. Then, for $y > |x|$ and $F(x, y) \neq 0$, we have

$$\begin{aligned} |F(x,y)| \geqslant \frac{|b|}{1.1} y^n \cdot \exp\left\{ -\left(\frac{2+\eta}{3} \cdot \frac{U^2}{\lambda} \log A + \frac{2(2+\eta)}{3} U + 1 \right) \log y \right\} \\ \cdot \exp\left\{ -\theta \left(1 + \frac{h}{\lambda} \right)^{3/2} (\log A \cdot \log y)^{1/2} \right\} \\ \cdot \exp\left\{ -3.04h - 2U \log A - 2.16 \log A \right\}, \end{aligned}$$

where

$$\lambda = \log\left(1 + \frac{\log A}{|\log(a/b)|}\right),$$

$$h = \max\left\{ 5\lambda, \log\lambda + 0.47 + \log\left(\frac{n}{\log A} + \frac{1.5}{\log\left(\max\{y, 3\}\right)} \right) \right\}$$

and

$$U = \frac{4h}{\lambda} + 4 + \frac{\lambda}{h}, \qquad \eta = \frac{1}{223}, \qquad \theta = \frac{16\sqrt{6(2+\eta)}}{3}.$$

To obtain good upper bounds upon n, we exploit some properties of a particular (Frey) elliptic curve corresponding to a putative solution to $ax^n - by^n = 1$. In effect, we consider such an equation to be a special case of a ternary equation of the form $ax^n - by^n = z^m$ for one of $m = 2$, $m = 3$ or $m = n$ (see, for example, [**3**], [**4**] or [**9**], respectively, for details on such equations). If $3 \mid b$, for example, we may, following [**4**], consider the curve

$$E : Y^2 + 3XY + bx^nY = X^3. \tag{6}$$

As it transpires, this is a good choice for E because the discriminant of E turns out to be of the form $2^\alpha 3^\beta m^n$ for integers α, β and m. By Theorem 3.1 and Lemma 3.2, we can suppose that $\gcd(y, 6) = 1$ (and, trivially for our choices of (a, b), that $|y| > 1$). We associate to the elliptic curve E, a (modular) Galois representation

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

on the n-torsion points $E[n]$ of E.

For $n \geqslant 5$ prime, by [**4**, Lemma 3.4], this representation arises from a weight 2 cuspidal newform

$$f = f_E = \sum_{n=1}^{\infty} c_n q^n,$$

of trivial character and level 54. Since all newforms at this level are one-dimensional, we see, for each prime $p \geqslant 5$, that $c_p = a_p$, where a_p is the pth Fourier coefficient of an elliptic curve of conductor 54. If $p \geqslant 5$ is a prime dividing y, then E has split multiplicative reduction at p and hence, via [**4**, Proposition 4.2], n necessarily divides $p + 1 - a_p$. It follows from the Hasse–Weil bounds that $n < p + 1 + 2\sqrt{p}$, and hence that $y + 1 + 2\sqrt{y} > n$, whereby

$$y > n - 2\sqrt{n}. \tag{7}$$

We will now employ Theorem 3.4 to deduce upper bounds upon n. Since (a, b) is $(1, 6)$, $(1, 12)$, $(1, 24)$ or $(3, 8)$, we may assume that $A = b$, and that

$$\lambda = \begin{cases} \log 2, & \text{in the first three cases,} \\ \log\left(1 + \dfrac{\log 8}{\log(8/3)}\right), & \text{if } (a, b) = (3, 8), \end{cases}$$

and

$$h = \log \lambda + 0.47 + \log\left(\frac{n}{\log b} + \frac{1.5}{\log y}\right).$$

Substituting these into Theorem 3.4 and using inequality (7) leads, after some routine calculations, to the conclusion that $|ax^n - by^n| > 1$ for positive integers x and y, provided that $n > n_0$ is prime, where n_0 is given as follows.

(a, b)	$(1, 6)$	$(1, 12)$	$(1, 24)$	$(3, 8)$
n_0	4831	6553	8269	5531

Note that, in the case $(a, b) = (3, 8)$, in order to employ the argument leading to (7), we have interchanged the roles of a and b.

We have thus shown that any equations of the shape (5) with (a, b) equal to $(1, 6)$, $(1, 12)$, $(1, 24)$ or $(3, 8)$, for which we have positive integral solutions with n prime, necessarily have $n \leqslant n_0$. In the next two sections, we will tackle these remaining equations.

4. *Solving high-degree binomial Thue equations*

We begin by presenting what might be considered a 'practical' method for completely resolving a given binomial Thue equation of the shape $ax^n - by^n = 1$, for arbitrary $n \geqslant 3$. In our situation, we will in fact restrict attention to prime exponents $n \geqslant 7$. For larger values of n, say $n > 100$, a traditional approach via linear forms in logarithms is impractical, due to the difficulty involved in computing systems of independent units in $\mathbb{Q}(\sqrt[n]{a/b})$, a necessary precondition for solving the given equation. Our method is rather different. If we actually have a positive solution (for example, if $a = 2$ and $b = 3$), then we may employ Theorem 3.3 to reach the desired conclusion. If not, we search for a local obstruction, by considering the equation modulo a prime of the form $p = 2kn + 1$, coprime to ab, for $k \in \mathbb{N}$. For such a prime, there are at most $2k + 1$ residue classes for x^n modulo p, and hence at most $(2k + 1)^2$ possible residue classes for $ax^n - by^n$ modulo p. If none of these is congruent to 1 modulo p, we derive a contradiction. For example, in our situation with $(a, b) = (3, 8)$ and prime n satisfying $5 \leqslant n \leqslant 5531$, we are able, in each case, to find such corresponding p, via a simple computation.

If $a = 1$, however, we must modify the above approach, as the solution $x = 1$, $y = 0$, ensures local solvability. In such a case, we will again consider $ax^n - by^n$ modulo a prime of the form $p = 2nk + 1$, coprime to ab. If the congruence

$$ax^n - by^n \equiv 1 \pmod{p} \tag{8}$$

implies that $p \mid xy$, then the relevant Frey curve E, corresponding to the putative solution (which may be slightly more complicated than that given in (6)), necessarily has multiplicative reduction (possibly not split) at p. Its corresponding mod p Galois representation ρ_E thus satisfies

$$\operatorname{trace} \rho_E(\mathrm{Frob}_p) = \pm(p+1),$$

whence, arguing as in the previous section and appealing to [**4**, Proposition 4.2], n divides

$$\mathrm{Norm}_{K/\mathbb{Q}}(p + 1 \pm c_p).$$

Here, c_p is the pth Fourier coefficient of a weight 2 cuspidal newform of level

$$N = 3^\delta \, \mathrm{Rad}(ab) = 3^\delta \prod_{p \mid ab} p$$

for some $-1 \leqslant \delta \leqslant 2$, where the form has coefficients in a number field K (again, see [**4**] for details of how to compute N precisely). If we find, after calculating these norms for each form at level N, that in all cases

$$\mathrm{Norm}_{K/\mathbb{Q}}(p + 1 \pm c_p) \not\equiv 0 \pmod{n},$$

then we reach the desired contradiction. In our situation, with $a = 1$ and $b \in \{6, 12, 24\}$, our curve is just that given in (6) whence, as in the previous section, we have split multiplicative reduction at p, and so

$$\operatorname{trace} \rho_E(\mathrm{Frob}_p) = p + 1,$$

whereby, as before,

$$a_p \equiv p + 1 \equiv 2 \pmod{n}, \tag{9}$$

where a_p is the pth Fourier coefficient of an elliptic curve of conductor 54. If this fails to occur, then we conclude as desired. In particular, if k is not too large, relative to n, say $k \leqslant (n-5)/8$, then the Hasse–Weil bounds imply that $|a_p| < n - 2$, and so we obtain a contradiction, unless $a_p = 2$. Note that for the two isogeny classes of elliptic curves over $\mathbb{Q}$ with conductor 54, the set of prime indices for which $a_p = 2$ is the same in either case: $p = 19, 37, 109, 757, \ldots$.

For example, let us consider $u^7 - 6v^7 = 1$. We take $p = 29$, and we note that $r^7 \equiv 0, \pm 1, \pm 12 \pmod{29}$ for integral r. It follows, if 29 fails to divide v, that

$$u^7 - 6v^7 \equiv \pm 2, \pm 3 \pm 5, \pm 6, \pm 7, \pm 11, \pm 13, \pm 14 \pmod{29},$$

and hence the equation $u^7 - 6v^7 = 1$ has no positive solutions in such a case. If, on the other hand, $v \equiv 0 \pmod{29}$, the fact that $c_{29} = \pm 6$ for the (two isogeny classes of) elliptic curves of conductor 54 contradicts identity (9) (where we have $p = 29$ and $n = 7$). It follows that the Diophantine equation $u^7 - 6v^7 = 1$ has no solutions in positive integers u and v.

We carry out this procedure for all primes $5 \leqslant n \leqslant n_0$, for the pairs $(a,b)=(1,6)$, $(a,b)=(1,12)$ and $(a,b)=(1,24)$. (The actual computation takes only a few minutes on a Sun Ultra 10; full data is available from the author on request.) In every case, we are able to find a prime $p = 2nk + 1$, from which we can conclude that (5) has no solutions in positive integers (x, y). These primes range from $23 \leqslant p \leqslant 432781$ (where this last value corresponds to $(a, b) = (1, 24)$ and $n = 7213$). In all but one case, the prime p is the smallest prime of the form $2nk+1$ for which the congruence (8) implies that $p \mid xy$. The only exception corresponds to the three cases where $n = 197$, and consideration of the equation

$$ax^{197} - by^{197} = 1$$

modulo 3547 implies that $p \mid xy$. Since $a_{3547} = 2$ for any elliptic curve of conductor 54, we cannot use this prime to conclude that the above equations are insoluble in positive integers. If, however, we consider these equations modulo $p = 4729$, we are led to the conclusion that $y \equiv 0 \pmod{4729}$, contradicting the fact that $a_{4729} = \pm 49$. This completes the proof of Theorem 1.2 in the case where $n \geqslant 7$ is prime.

5. *Solving low-degree binomial Thue equations*

To finish the proof of Theorem 1.2, it remains to solve all possible Thue equations of the shape (5) with $ab = 2^\alpha 3^\beta$ and $n \in \{3, 4, 5\}$. We may assume, without loss of generality, that a and b are positive, coprime integers with $a < b$, $ab = 2^\alpha 3^\beta$ and $0 \leqslant \alpha, \beta \leqslant n - 1$. For $n = 3$, this leaves us with precisely twelve equations of the shape $ax^3 - by^3 = 1$ to solve. For $n = 4$, we have twenty-four equations of the form $ax^4 - by^4 = 1$, and a like number of the form $ax^4 - by^4 = -1$. Finally, for $n = 5$, Theorem 3.1 and Lemma 3.2 imply that we may suppose that $\beta = 1$ and $\alpha \in \{1, 2, 3\}$. Local considerations modulo 9, 11 and 16, together with Theorem 3.3, reduce the problem, in all cases, to that of solving the equations $x^n - 2^\alpha 3^\beta y^n = 1$, which we do via standard techniques based on lower bounds for linear forms in logarithms in conjunction with lattice basis reduction. We may, for example, employ the computational package Kant. For forms of such low degree and height, this is nowadays a relatively routine matter (though this is by no means the case for even moderately large values of n). In conclusion, the only solutions that we encounter are those corresponding to

$$(a, b, n) = \begin{cases} (1, 2, n), \\ (2, 3, n), \\ (3, 4, n), \\ (8, 9, n), \\ (1, 9, 3). \end{cases}$$

This concludes the proof of Theorem 1.2.

6. *Proof of Corollary* 1.4

We now turn our attention to the corollaries of Theorem 1.1. Let us begin by supposing that $x^2 - Dy^n = -1$, for x and y positive integers, $D = 2^\alpha 3^\beta$ with α and β nonnegative integers, and $n \geqslant 3$ an integer. Since D divides $x^2 + 1$, we necessarily have $\beta = 0$. If $n \geqslant 7$ is prime, then, from [**3**, Theorem 1.2], we conclude that $\alpha = 1$. In this case, work of Størmer [**17**] and Ljunggren [**11**] allows us to conclude that $x = y = 1$, or that $x = 239$, $y = 13$ and $n = 4$.

Let us next suppose that $x^2 - Dy^n = 1$, for x and y positive integers, $D = 2^\alpha 3^\beta$ with α and β nonnegative, and $n \geqslant 3$. It follows that

$$(x-1)(x+1) = 2^\alpha 3^\beta y^n$$

and so, from Theorem 1.1, $x \in \{2, 3, 5, 7, 17\}$.

This completes the proof of Corollary 1.4.

7. *Proof of Corollary* 1.5

To prove Corollary 1.5, we begin by supposing that we have positive integers m, t, b and n, with $2 \leqslant t \leqslant 4$ and

$$(m + d_1)(m + d_2) \ldots (m + d_t) = by^n,$$

where $0 \leqslant d_1 < d_2 < \ldots < d_t \leqslant t$, $P(b) \leqslant t + 1$ and (so that we may apply Theorem 1.1) $n \geqslant 3$. Writing $m + d_i = a_i y_i^n$, where a_i is nth-power-free, we consider the set S, consisting of integers d_i for which $P(a_i) \leqslant 3$. Corollary 1.5 will follow from Theorem 1.1 (after some rather benign calculations) if we can show that S necessarily contains two distinct elements d_i and d_j for which $d_i - d_j = 2^\alpha$ for some nonnegative integer α.

We may view this as a graph-theoretic problem. Given $k \geqslant t$ and m, write, for each i with $0 \leqslant i \leqslant k-1$, $m + i = c_i e_i$ where $P(c_i) \leqslant k$ and e_i is coprime to $\prod_{p \leqslant k} p$. We define a graph S_m to consist of vertices i for which $P(c_i) \leqslant 3$. We connect two vertices of S_m with an edge if they differ by a nonnegative power of 2. Notice that S_m depends only on the residue class of m modulo $\prod_{5 \leqslant p \leqslant k} p$. It is thus a finite computation to determine, for each k, the minimal number of vertices $i \in S_m$ that need be removed to totally disconnect the graph S_m.

For example, if $k = 3$, then $S_m = \{0, 1, 2\}$ for each m, and so we would need to remove at least two vertices to disconnect S_m. This implies that Corollary 1.5 holds in the case where $t = 2$. Similarly, $k = 4$ implies that $S_m = \{0, 1, 2, 3\}$, again requiring two removed vertices (whence Corollary 1.5 holds for $t = 3$). Finally, if $k = 5$, then

$$S_m = \begin{cases} \{1,2,3,4\}, & \text{if } m \equiv 0 \pmod 5, \\ \{0,1,2,3\}, & \text{if } m \equiv 1 \pmod 5, \\ \{0,1,2,4\}, & \text{if } m \equiv 2 \pmod 5, \\ \{0,1,3,4\}, & \text{if } m \equiv 3 \pmod 5, \\ \{0,2,3,4\}, & \text{if } m \equiv 4 \pmod 5, \end{cases}$$

again requiring the removal of at least two vertices to disconnect. This completes the proof of Corollary 1.5 in the case where $n \geqslant 3$.

We note that this argument may be easily extended to deal with larger values of k (and, indeed, of $k - t$; we may, for example, treat $k - t = 2$, provided that $t \geqslant 7$). In such a situation, the number of cases for S_m grows quite quickly (exponentially in k) and, though it an easy matter to generate the graphs S_m for a value of k from those corresponding to $k - 1$, we are nonetheless restricted to relatively small k.

To handle equation (2) with $n=2$, we note that the elliptic equations corresponding to

$$(m+1)(m+d_2)(m+d_3) = 2^\alpha 3^\beta y^2, \qquad 0 = d_1 < d_2 < d_3 \leqslant 3,$$

and

$$(m+d_1)(m+d_2)(m+d_3)(m+d_4) = 2^\alpha 3^\beta 5^\gamma y^2, \qquad 0 = d_1 < d_2 < d_3 < d_4 \leqslant 4$$

(where we may suppose that $\alpha, \beta, \gamma \in \{0,1\}$), are easily solved via, say, lower bounds for linear forms in elliptic logarithms. (In fact, in many cases, elementary arguments suffice.) Such an approach is implemented in the computational package Simath. Employing this, we find only the positive solutions m given in the statement of Corollary 1.5, completing the proof. Alternatively, we can obtain this result by utilizing a lower bound for simultaneous rational approximation to $\sqrt{2}$ and $\sqrt{3}$ of the shape

$$\max\left\{\left|\sqrt{2} - \frac{p_1}{q}\right|, \left|\sqrt{3} - \frac{p_2}{q}\right|\right\} > 10^{-10} q^{-1.8161},$$

valid for positive integers p_1, p_2 and q (see [**1**] for details). This enables one to show that integer solutions to the simultaneous equations

$$x^2 - 2z^2 = u, \qquad y^2 - 3z^2 = v,$$

satisfy

$$\max\{|x|, |y|, |z|\} \leqslant \left(10^{10} \max\{|u|, |v|\}\right)^{5.5}. \tag{10}$$

To see how such a result may be of use in solving equation (2) with $n = 2$, suppose, by way of example, that

$$m(m+2)(m+3) = 3y^2,$$

for positive integers m and y. It follows that either $m = 1$ and $y = 2$, or that there exist positive integers a, b and c such that

$$m = 6a^2, \qquad m+2 = 2b^2, \qquad m+3 = c^2,$$

whereby

$$c^2 - 2b^2 = 1, \qquad (3a)^2 - 3b^2 = -3.$$

Inequality (10) thus implies that $c < 10^{58}$. A quick check of convergents in the continued fraction expansion of $\sqrt{2}$ shows that $(a, b, c) = (1, 2, 3)$. The other remaining cases follow in a similar fashion.

Acknowledgments. The author would like to thank the anonymous referee for insightful comments and – particularly – for correcting a number of computational errors.

References

1. M. A. Bennett, 'Simultaneous approximation to pairs of algebraic numbers', *Canad. Math. Soc. Proceedings* 15 (1995) 55–65.

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

4. M. A. Bennett, V. Vatsal and S. Yazdani, 'Ternary Diophantine equations of signature $(p, p, 3)$', *Compositio Math.*, to appear.

5. H. Darmon and L. Merel, 'Winding quotients and some variants of Fermat's last theorem', *J. Reine Angew. Math.* 490 (1997) 81–100.

6. P. Erdős and J. Selfridge, 'The product of consecutive integers is never a power', *Illinois J. Math.* 19 (1975) 292–301.

7. K. Győry, 'On the Diophantine equation $n(n+1)\dots(n+k-1) = bx^l$', *Acta Arith.* 83 (1998) 87–92.

8. G. Hanrot, N. Saradha and T. N. Shorey, 'Almost perfect powers in consecutive integers', *Acta Arith.* 99 (2001) 13–25.

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

10. W. Ljunggren, 'Einige Eigenschaften der Einheiten reeler quadratischer und rein biquadratischer Zahlkörper', *Oslo Vid-Akad Skrifter* 1 (1936) 12.

11. W. Ljunggren, 'Zur Theorie der Gleichung $x^2 + 1 = Dy^4$', *Avh. Norske Vid. Akad. Oslo* 5 (1942).

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

13. P. Ribenboim, *Catalan's conjecture* (Academic Press, NY, 1994).

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

15. N. Saradha, 'On perfect powers in products with terms from arithmetic progressions', *Acta Arith.* 82 (1997) 147–172.

16. E. Selmer, 'The diophantine equation $ax^3 + by^3 + cz^3 = 0$', *Acta Math.* 85 (1951) 203–362.

17. C. Størmer, 'Solution complète en nombres entiers de l'équation $m \operatorname{arc\,tang} 1/x + n \operatorname{arc\,tang} 1/y = k\pi/4$', *Bull. Soc. Math. France* 27 (1899) 160–170.

18. N. Tzanakis, 'The complete solution in integers of $x^3 + 3y^3 = 2^n$', *J. Number Theory* 19 (1984) 203–208.

19. N. Tzanakis and B. M. M. de Weger, 'How to explicitly solve a Thue–Mahler equation', *Compositio Math.* 84 (1992) 223–288.

Michael A. Bennett
Department of Mathematics
University of British Columbia
Vancouver, B.C., V6T 1Z2
Canada

bennett@math.ubc.ca