ACTA ARITHMETICA
184.1 (2018)

Powers from products of k terms in progression: finiteness for small k

by

Michael A. Bennett (Vancouver)

Dedicated to Rob Tijdeman on the occasion of his 75th birthday, with many more to come!

1. Introduction. A striking result of Erdős and Selfridge [8] is that the Diophantine equation

$$n(n+1)\cdots(n+k-1) = y^\ell$$

has no solution in positive integers n, k, y and ℓ with $\min\{k, \ell\} \geq 2$. Attempts to derive an analogous statement for the equation

$$n(n+d)\cdots(n+(k-1)d) = y^\ell, \tag{1.1}$$

where a similar nonexistence of solutions has been conjectured by Erdős to hold for n, d positive and coprime and k suitably large, have led to a large number of interesting conditional results (see e.g. [11], [14], [15], [18]–[20], [22], [25]–[27]). For fine surveys of the extensive literature on this problem, the reader is directed to Győry [9], Shorey [23], [24] and Tijdeman [28].

Very recently, the author, jointly with Siksek [2], proved that, for fixed $k \geq k_0$, equation (1.1) has only finitely many solutions (where $n, d, y \neq 0$ and $\ell \geq 2$ are variable, and $\gcd(n, d) = 1$). While k_0 here is effectively computable, it is not explicitly determined in [2], but certainly exceeds e^{10^6}.

For small values of k, finiteness results for (1.1) (under coprimality assumptions) have been obtained for $k \leq 82$ in [1, Theorem 1.4] and, in completely explicit form for $k \leq 34$, in [10]. The techniques of [1] do not allow for substantial strengthening of these results, however. The goal of the paper at hand is to considerably extend [1, Theorem 1.4] using techniques from [2] and a variety of new ideas. We prove

2010 *Mathematics Subject Classification*: Primary 11D41, 11G05.
Key words and phrases: Diophantine equation.
Received 6 November 2017.
Published online 8 February 2018.

DOI: 10.4064/aa171106-19-12

THEOREM 1.1. *There exist at most finitely many integers n, d, y, ℓ and k with $\gcd(n,d)=1$, $\ell \geq 2$ and $4 \leq k \leq 15177$ for which equation (1.1) is satisfied.*

The outline of this paper is as follows. In Section 2, we derive two results by associating certain *Frey–Hellegouarch* curves to solutions to (1.1). In Sections 3–5, we detail a number of combinatorial identities that will provide us with a powerful tool for applying the results of Section 2. Finally, in Section 6, we combine these techniques to prove Theorem 1.1, through the addition of explicit bounds for the size of sets without 3-term arithmetic progressions, and complete solutions of certain S-unit equations due to von Känel and Matschke [12].

2. Applications of the modular method. If we have a solution to (1.1) in coprime nonzero integers, we can write

$$n + id = b_i y_i^{\ell}, \tag{2.1}$$

where $P(b_i)$, the greatest prime factor of b_i, satisfies $P(b_i) < k$ and we may assume that each b_i is ℓth power free. Our goal is to use this information to find integers A, B, C, a, b and c for which

$$Aa^{\ell} + Bb^{\ell} = Cc^{m}, \quad m \in \{2, 3, \ell\}, \tag{2.2}$$

where we can guarantee the existence of a prime p which divides ab, while failing to divide $6ABC$. If we can accomplish this, we will bound ℓ as follows.

PROPOSITION 2.1. *Let A, B and C be nonzero coprime integers and ℓ be prime. For $m \in \{2, 3, \ell\}$, define $\kappa_m = \kappa_m(C)$ by*

$$\kappa_m = \begin{cases} 2^5 & \text{if } m = \ell, \\ 2^7 \prod_{q \mid C} q & \text{if } m = 2, \\ 3^4 \prod_{q \mid C} q & \text{if } m = 3, \end{cases}$$

where the products are over prime values of q. If there exist nonzero integers a, b and c satisfying (2.2) and a prime p, relatively prime to $6ABC$, for which $p \mid ab$, then

$$\ell \leq (\sqrt{p} + 1)^{(1 + \kappa_m \prod_{q \mid ABC} q)/6}. \tag{2.3}$$

Proof. If we suppose we have such a solution to (2.2), then, by combining results from [3], [4] and [13], there exists a cuspidal newform $f = \sum_{n \geq 1} c_n q^n$ of weight 2 and level N, where

$$N \mid \kappa_m \prod_{q \mid ABC} q.$$

Furthermore, since we assume that $p \mid ab$ and $p \nmid 6ABC$, we have

$$p + 1 \equiv \pm c_p \pmod{\lambda}, \tag{2.4}$$

where $\lambda \mid \ell$ is a prime in the totally real field $K = \mathbb{Q}(c_1, c_2, \ldots)$.

We thus have

$$\ell \mid \mathrm{Norm}_{K/\mathbb{Q}}(p+1 \mp c_p),$$

and hence, as c_p is bounded by $2\sqrt{p}$ in all the real embeddings of K, via the Hasse–Weil theorem,

$$\ell \leq (p+1+2\sqrt{p})^{[K:\mathbb{Q}]} = (\sqrt{p}+1)^{2[K:\mathbb{Q}]}.$$

Denoting the dimension of $S_2^{\mathrm{new}}(N)$ by $g_0^+(N)$, we thus have $[K:\mathbb{Q}] \leq g_0^+(N)$, whereby, since Theorem 2 of Martin [16] implies that

$$g_0^+(N) \leq \frac{N+1}{12},$$

we deduce inequality (2.3), as desired. ∎

To apply this result, we must show that a solution to (1.1), under certain hypotheses at least, necessarily implies the existence of integers A, B, C, a, b, c, $m \in \{2,3,\ell\}$ and p prime, such that $p \mid ab$, $p \nmid ABCc$ and p is bounded as a function of k. To do this, we will appeal to a number of polynomial identities which we will deduce in the next three sections.

Additionally, in case we are not able to guarantee the existence of such a p (or to bound its size), we will have use of the following.

PROPOSITION 2.2. *Suppose that $k \geq 4$, n, d, y, ℓ is a solution to* (1.1) *with* $\gcd(n,d) = 1$ *and prime ℓ satisfying* $\log \ell \geq 3^k$, *and* $\{i, i+j, i+2j\}$ *is a nontrivial* 3*-term arithmetic progression of indices in* $\{0,1,\ldots,k-1\}$. *Define an elliptic curve E_0 (given in Cremona's tables* [5] *as* 32a2) *by*

$$E_0 : \ y^2 = x^3 - x.$$

Then there exists an elliptic curve $E/\mathbb{Q}$ with full rational 2*-torsion, without complex multiplication, and with conductor N_E dividing* $16R$, *where*

$$R = \mathrm{Rad}(b_i b_{i+j} b_{i+2j}),$$

and the b_t are as defined in (2.1). *If we further assume that p is a prime for which $p \mid d$ and $\ell > 4\sqrt{p}$, then*

$$a_p(E) = \pm a_p(E_0).$$

In particular, if $p \equiv 3 \pmod 4$, *then* $a_p(E) = 0$.

Proof. From [10], we may suppose that $k \geq 35$. Arguing as in [2, proof of Lemma 5.1] and appealing to [13, Théorème 4], we see that if

$$\ell > \left(1 + \sqrt{\frac{8}{3} R \log R \exp(0.27 + 5/\log R)}\right)^{(16R+1)/12}, \tag{2.5}$$

then there exists a curve E of conductor $N_E \mid 16R$, with full rational 2-torsion, for which

$$a_p(E) = \pm a_p(F) \pmod \ell,$$

for each prime p that fails to divide $(n+id)(n+(i+j)d)(n+(i+2j)d)$, where the elliptic curve F is defined via

$$F:\ y^2 = x(x-n-id)(x+n+(i+2j)d).$$

Since

$$R \le \prod_{q \le k} q < e^{1.000081k},$$

where the last inequality is a consequence of work of Schoenfeld [21], the right hand side of (2.5) is readily seen to be bounded above by e^{3^k}, provided $k \ge 33$. If $p \mid d$, we thus have $a_p(F) = \pm a_p(E_0)$ (since the curve given by the model $y^2 = x^3 - n^2x$ is a quadratic twist of E_0). It follows that

$$a_p(E) = \pm a_p(E_0) \pmod{\ell},$$

whence $a_p(E) = \pm a_p(E_0)$ via the Hasse–Weil bounds, since we assume $\ell > 4\sqrt{p}$. The fact that the curve E does not have complex multiplication (which eliminates the possibility that $R = 2$) is a consequence of [2, proof of Proposition 6.1]. The additional fact that $a_p(E) = 0$ for $p \equiv 3 \pmod 4$ is classical. ∎

3. Combinatorial identities

3.1. Notation. Let j be a positive integer. Denote by

$$\{a_1, \ldots, a_j; b_1, \ldots, b_j; c_1, \ldots, c_j\}$$

three j-tuples of integers with the property that there exist integers α, β and γ, not all zero, satisfying the polynomial identity

$$\alpha \prod_{i=1}^{j}(x+a_i) + \beta \prod_{i=1}^{j}(x+b_i) + \gamma \prod_{i=1}^{j}(x+c_i) = 0. \tag{3.1}$$

Further, by

$$[a_1, \ldots, a_j; b_1, \ldots, b_j]$$

we mean two distinct j-tuples of integers satisfying the polynomial identity

$$\prod_{i=1}^{j}(x+a_i) - \prod_{i=1}^{j}(x+b_i) = \prod_{i=1}^{j} a_i - \prod_{i=1}^{j} b_i. \tag{3.2}$$

Henceforth, we will write $\nu_p(m)$ for the largest integer j such that p^j divides a nonzero integer m.

3.2. Primes dividing $n+id$ for precisely one value of i. Let us begin by supposing that p divides precisely one of the terms

$$n, n+d, \ldots, n+(k-1)d,$$

say $p \mid n+id$. This is certainly the case if $p \mid y$ in (1.1) and $p \geq k$ (and possibly the case if $p \mid y$ and $k/2 < p < k$). Then one of $\{i-2; i-1; i\}$ or $\{i; i+1; i+2\}$ (which each give (3.1) with $(\alpha, \beta, \gamma) = (1, -2, 1)$) consists entirely of indices in $\{0, 1, \ldots, k-1\}$. Writing $x = n/d + i$ thus leads to an equation of the shape (2.2) with $m = \ell$, $P(ABC) < k$, $p \mid ab$ and $p \nmid 6ABC$.

3.3. Primes dividing $n+id$ for precisely two values of i. If a prime p divides precisely two of the terms

$$n, n+d, \ldots, n+(k-1)d,$$

then we may assume that $p \mid n+id$ and $p \mid n+(i+p)d$, where $0 \leq i \leq k-p-1$. In this case, we consider the tuple

$$\{0, p; b_1, b_2; c_1, c_2\}.$$

In order for there to exist a nontrivial polynomial identity of the shape (3.1), where we wish to have

$$0 < b_1, b_2, c_1, c_2 < p,$$

it is necessary that

$$\begin{vmatrix} 1 & 1 & 1 \\ p & b_1+b_2 & c_1+c_2 \\ 0 & b_1b_2 & c_1c_2 \end{vmatrix} = 0.$$

This is obviously easy to arrange by taking, for instance,

$$b_1 = 1, \quad b_2 = p-1, \quad c_1 = 2, \quad c_2 = p-2,$$

which are all distinct from 0 and p, provided $p \geq 5$, corresponding to (3.1) with

$$\alpha = \frac{p-3}{2}, \quad \beta = 2-p \quad \text{and} \quad \gamma = \frac{p-1}{2}.$$

Once again, we are led to a solution to (2.2) with $m = \ell$, $P(ABC) < k$, $p \mid ab$ and $p \nmid 6ABC$.

3.4. First conclusions. From the preceding subsections, we have the following (which is essentially contained in [1, proof of Theorem 1.5]; see also [2, Lemma 4.1]).

LEMMA 3.1. *If $k \geq 4$, n, d, ℓ is a nontrivial solution to* (1.1)*, and $k/2 < p \leq k$ is prime, then either $p \mid d$ or*

$$\log \ell < 3^k.$$

Proof. As before, we may suppose that $k \geq 35$. If $p \leq k$ is prime then either $p \mid d$, or

$$p \mid n(n+d)\cdots(n+(k-1)d).$$

Since we assume that (1.1) is satisfied, if $p \nmid d$ it follows from $k/2 < p \le k$ that p divides either one or two of the terms

$$n, n+d, \dots, n+(k-1)d.$$

From our preceding arguments, in either case, we find a nontrivial solution to an equation of the shape (2.2) with $m = \ell$, $P(ABC) < k$, $p \mid ab$ and $p \nmid 6ABC$. Dividing through by suitable common factors, we appeal to Proposition 2.1. Since

$$\prod_{q \mid ABC} q \le \prod_{q<k} q,$$

where the latter product is over all primes less than k, we deduce, via Schoenfeld [21], that

$$\prod_{q \mid ABC} q < e^{1.000081k},$$

and hence, from (2.3) and the fact that $p \le k$,

$$\ell < (\sqrt{k}+1)^{1/6+(16/3)e^{1.000081k}} < e^{3^k},$$

where the last inequality is valid for all $k \ge 23$. ∎

4. Primes dividing $n+id$ for precisely three values of i. We suppose next that we have a nontrivial solution to (1.1) and that p is a prime such that there exist precisely three indices $i \in \{0, 1, \dots, k-1\}$ for which $n+id$ is divisible by p, say

$$p \mid n+id, \quad p \mid n+(i+p)d \quad \text{and} \quad p \mid n+(i+2p)d.$$

Note for future use that since we assume $\ell \ge 4$, p^2 divides precisely one of $n+id$, $n+(i+p)d$ or $n+(i+2p)d$.

We would like to argue as in the preceding section, by finding a tuple of the shape $\{0, p, 2p; b_1, b_2, b_3; c_1, c_2, c_3\}$, with the b_i and c_i positive integers, each coprime to p and lying in the interval $(0, 2p)$. If the corresponding coefficients α, β and γ in (3.1) are also coprime to p, then we can apply Proposition 2.1 to deduce an upper bound upon ℓ. It is a finite computation to verify the existence of such identities, for a given value of p, and we can confirm that there exist identities with the desired properties for each prime p with $11 \le p < 500$. It seems likely that such an identity in fact exists for every $p \ge 11$. We will not, however, prove this, rather choosing to approach the problem somewhat differently.

If $p^2 \mid n+(i+p)d$, then it follows that

$$\nu_p(b_{i+p}) = \ell - 2 \quad \text{and} \quad \nu_p(b_i) = \nu_p(b_{i+2p}) = 1.$$

We consider the tuple

$$\{0, 0, p; 1, 2p-2, 2p-2; 2, 2, p-1\},$$

corresponding to the identity

$$(p-2)x^2(x+p)+(x+1)(x+2p-2)^2=(p-1)(x+2)^2(x+p-1).$$

Writing as before $x = n/d + i$, we thus have a solution to (2.2) with, from (2.1),

$$A=(p-2)\frac{b_i^2 b_{i+p}}{p^\ell},\quad B=b_{i+1}b_{i+2p-2}^2,\quad C=(p-1)b_{i+2}^2 b_{i+p-1},$$
$$a=py_i^2y_{i+p},\qquad b=y_{i+1}y_{i+2p-2}^2,\quad c=y_{i+2}^2y_{i+p-1}$$

and $m = \ell$. After dividing through by any common factors, we once again have a solution to (2.2) with coprime coefficients A, B and C each composed of primes factors smaller than k, $p\nmid ABC$ and $p \mid ab$.

For the remainder of this section, we may therefore suppose that

$$p \parallel n+(i+p)d.$$

We will handle this situation by considering the cases $p \equiv -1 \pmod{12}$, $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$ separately.

4.1. $p \equiv -1 \pmod{12}$**.** In this case, let us begin by noting that Theorem 112 of Nagell [17] guarantees the existence of positive integers r and s such that $p = 3r^2 - s^2$, where $\max\{r, s\} < \sqrt{p/2}$. We claim that $r > s$: if not, then

$$p=3r^2-s^2<2s^2<p,$$

an immediate contradiction. The tuple

$$\{0,p,2p;b_1,b_2,b_3;c_1,c_2,c_3\}$$

with

$$b_1=s(r-s),\quad b_2=(r+s)(3r-2s),\quad b_3=2r(3r-s),$$
$$c_1=2s(r-s),\quad c_2=2r(3r-2s),\quad c_3=(r+s)(3r-s)$$

thus corresponds to an identity of the shape (3.1) with $\alpha = \gamma = 1$ and $\beta = -2$. Here, the assumption $r > s$ ensures that

$$0<s(r-s)=b_1<r^2<3r^2-s^2=p,$$

and, in fact, it is easy to show that

$$0<b_1<c_1<p<b_2<c_2,c_3<b_3<2p.$$

A short check that we cannot have $c_2 = c_3$ completes the construction (i.e. ensures that the b_i and c_i are distinct indices in the interval $(0, 2p)$, each coprime to p). We are thus led, once more, to an equation of the shape (2.2) with $m = \ell$, $P(ABC) < k$, $p \mid ab$ and $p\nmid 6ABC$.

We can, in fact, employ an almost identical argument in case $p \equiv 1 \pmod{12}$, using the fact that such primes may be represented by the quadratic form $r^2 - 3s^2$.

4.2. $p \equiv 1 \pmod 4$**.** Here, there exist unique positive integers r and s such that $r > s$ and $p = r^2+s^2$. If $p^2 \mid n+id$, we note the polynomial identity

$$s(r-s)(x+2r^2)(x+(r+s)^2)+px(x+p) = r(r+s)(x+r^2-s^2)(x+2rs),$$

corresponding to the tuple

$$\{0, p; 2r^2, (r+s)^2; r^2-s^2, 2rs\}.$$

From the fact that $p = r^2+s^2$ with $r > s$ positive, it follows that

$$0 < 2r^2, (r+s)^2, r^2-s^2, 2rs < 2p$$

and that p fails to divide any of $2r^2, (r+s)^2, r^2-s^2$ and $2rs$. We thus have

$$0 < 2r^2+i, (r+s)^2+i, r^2-s^2+i, 2rs+i < k-1.$$

We apply this, as previously, with $x = n/d+i$, multiplying through by d^2, to again obtain a solution to (2.2) with $m = \ell$, $P(ABC) < k$, $p \mid ab$ and $p \nmid 6ABC$.

Analogously, when $p \parallel n+id$, the tuple

$$\{p, 2p; 2s^2, (r-s)^2; r^2+3s^2, 2(r^2+s^2-rs)\}$$

corresponds to an identity of the shape (3.1) with

$$\alpha = p, \quad \beta = s(r-s) \quad \text{and} \quad \gamma = -r(r+s),$$

and hence leads to a like conclusion.

4.3. $p \equiv 1 \pmod 3$**.** In this remaining case, we will instead appeal to identities corresponding to tuples of the shape $[a_1, a_2, a_3; b_1, b_2, b_3]$. For such primes, we may (following classical work of Fermat) write $p = r^2+3s^2$, whereby we have the tuple

$$[p, p, 2p; b_1, b_2, b_3]$$

with

$$b_1 = r^2-2rs+5s^2, \quad b_2 = r^2+2rs+5s^2 \quad \text{and} \quad b_3 = 2(r^2+s^2).$$

This corresponds to the fact that

$$(x+p)^2(x+2p)-(x+b_1)(x+b_2)(x+b_3) = 4s^2(r^2-s^2)^2. \tag{4.1}$$

We also have

$$[0, p, p; b_1, b_2, b_3],$$

where

$$b_1 = (r+s)^2, \quad b_2 = (r-s)^2 \quad \text{and} \quad b_3 = 4s^2,$$

corresponding to

$$x(x+p)^2-(x+b_1)(x+b_2)(x+b_3) = -4s^2(r^2-s^2)^2. \tag{4.2}$$

Yet again we write $x = n/d+i$ and multiply (4.1) and (4.2) through by d^3 to obtain equations of the shape (2.2) with $m = 3$, $P(AB) < k$

and $C = 4s^2(r^2 - s^2)^2$, where

$$s < \sqrt{p/3} < \sqrt{k/6} \quad \text{and} \quad |r^2 - s^2| < p < k/2. \tag{4.3}$$

In the case corresponding to (4.1), we have $p \,|\, ab$ and $p \nmid ABC$ precisely when $p^2 \,|\, n + (i + 2p)d$, while in the case corresponding to (4.2), we see that $p \,|\, ab$ and $p \nmid ABC$ when $p^2 \,|\, n + id$.

4.4. Conclusions. We thus have

LEMMA 4.1. *If $k \geq 4$, n, d, ℓ is a nontrivial solution to* (1.1)*, and $k/3 < p \leq k$ is prime, then either $p \,|\, d$ or*

$$\log \ell < 4^k.$$

Proof. Suppose that $p \nmid d$. From Lemma 3.1, we may also suppose that $k/3 < p \leq k/2$ and

$$p \,|\, n(n + d) \cdots (n + (k - 1)d),$$

so that p divides either two or three terms among

$$n, n + d, \ldots, n + (k - 1)d.$$

If we are led to a solution to (2.2) with $m = \ell$, $P(ABC) < k$, $p \,|\, ab$ and $p \nmid 6ABC$, then we argue precisely as in the proof of Lemma 3.1 to conclude that $\log \ell < 3^k$. If, however, we are led to a solution to (2.2) with $m = 3$, $P(AB) < k$, $C = 4s^2(r^2 - s^2)^2$, $p \,|\, ab$ and $p \nmid 6ABC$, then we apply Proposition 2.1 to conclude that

$$\ell \leq (\sqrt{p} + 1)^{(1+81 \prod_{q|C} q^2 \prod_{q|AB} q)/6}.$$

Since [21] and (4.3) imply that

$$\log\Big(\prod_{q|C} q^2 \prod_{q|AB} q\Big) \leq \log(2|s|\,|r^2 - s^2|) + \sum_{q \leq k} \log q < 1.000081k + 1.5 \log k,$$

after a little work we conclude as desired (since we may assume that $k \geq 35$). Note here that the upper bound $\log \ell < 4^k$ may be sharpened to $\log \ell < 3^k$ provided we assume that $k \geq 105$. ∎

5. Primes dividing $n+id$ for precisely four values of i. The last case we will consider in this paper is when we have a nontrivial solution to (1.1) and a prime p such that there exist precisely four indices $i \in \{0, 1, \ldots, k-1\}$ for which $n + id$ is divisible by p, say

$$p \,|\, n + id, \quad p \,|\, n + (i + p)d, \quad p \,|\, n + (i + 2p)d, \quad p \,|\, n + (i + 3p)d.$$

In this situation, we will suppose further that $p \equiv 1 \pmod 4$ and $p > 5$, so that we can write $p = r^2 + s^2$ with r and s positive integers, say $r < s$. We appeal to the identity corresponding to

$$[0, p, 2p, 3p; b_1, b_2, b_3, b_4],$$

where we set

$$(b_1, b_2) = \begin{cases} (rs + 3s^2, r^2 - 3rs + 2s^2) & \text{if } s < 3r, \\ (rs + 3r^2, s^2 - 3rs + 2r^2) & \text{if } s > 3r, \end{cases}$$

$b_3 = 3p - b_1$ and $b_4 = 3p - b_2$. We check that, with these choices, we have both $0 < b_i < 3p$ and $\gcd(b_i, p) = 1$, for each $i \in \{1, 2, 3, 4\}$ (this last condition requires the assumption that $p > 5$).

From the identity

$$(x + b_1)(x + b_2)(x + b_3)(x + b_4) - x(x + p)(x + 2p)(x + 3p) = b_1 b_2 b_3 b_4,$$

we argue as previously, setting $x = n/d + i$ and multiplying through by d^4 to obtain an equation of the shape (2.2) with $m = 2$, $P(AB) < k$, $|C| < k^4$, $P(C) < \sqrt{k}$, $p \mid ab$ and $p \nmid ABC$. We thus have

LEMMA 5.1. *If $k \geq 4$, n, d, ℓ is a nontrivial solution to* (1.1)*, and $k/4 < p \leq k/3$ is prime with $p \equiv 1 \pmod 4$, then either $p \mid d$ or*

$$\log \ell < 5^k.$$

Proof. If $k/4 < p \leq k/3$ and $p \nmid d$, then p divides either three or four of the terms in

$$n, n + d, \ldots, n + (k - 1)d.$$

As before, we apply Proposition 2.1 to conclude that

$$\ell \leq (\sqrt{p} + 1)^{(1 + 128 \prod_{q \mid C} q^2 \prod_{q \mid AB} q)/6}$$

and appeal to the inequalities $p < k/3$ and

$$\log\Big(\prod_{q \mid C} q^2 \prod_{q \mid AB} q\Big) \leq 4 \log k + \sum_{q \leq k} \log q < 1.000081k + 4 \log k.$$

The desired result is a consequence of the fact that $k \geq 28$. If we assume that $k \geq 267$, we may replace the bound $\log \ell < 5^k$ by $\log \ell < 3^k$. ∎

6. Computational finiteness. We now proceed with the proof of Theorem 1.1. Suppose that we have a nontrivial solution to (1.1), where, from [1, Theorem 1.4], we may assume that $k \geq 83$. By Lemmata 4.1 and 5.1, if $\log \ell \geq 5^k$, then necessarily $p \mid d$ for every prime p with $k/3 < p \leq k$ and for every prime $p \equiv 1 \pmod 4$ with $k/4 < p \leq k/3$. We claim that, for $83 \leq k \leq 15177$, we can find a nontrivial 3-term arithmetic progression $\{i, i + j, i + 2j\}$ (i.e. with $j \neq 0$) of indices in $\{0, 1, \ldots, k - 1\}$ such that

$$P(b_i b_{i+j} b_{i+2j}) \leq 53. \tag{6.1}$$

Notice that, for $k \leq 177$, Lemma 4.1 ensures that $P(b_i) \leq 53$ for all i, and hence such a result is immediate for such k (taking the indices $\{0, 1, 2\}$ for example). To see this for larger k, note that the number of indices i for which we can have $p \mid b_i$ for a given prime p is at most $[(k - 1)/p] + 1$. It follows

that the number of indices $i \in \{0, 1, \dots, k-1\}$ such that $P(b_i) \le 53$ is at least

$$k - \sum_{59 \le p < k/4} \left(\left[\frac{k-1}{p} \right] + 1 \right) - \sum_{\substack{k/4 \le p < k/3 \\ p \equiv 3 \pmod 4}} \left(\left[\frac{k-1}{p} \right] + 1 \right), \tag{6.2}$$

where the sum is over prime p. A short computation reveals that this exceeds $0.27k$ for all $k \le 15177$.

We next have need of a computational result on the size $r(N)$ of the largest subset S of

$$S_N = \{1, \dots, N\}, \quad N \in \mathbb{N},$$

that fails to contain a nontrivial 3-term arithmetic progression. Work of Dybizbański [7] implies that we have

N	$r(N)$	N	$r(N)$	N	$r(N)$
1	1	30, 31	12	82, 83	23
2, 3	2	32, 33, 34, 35	13	84, 85, ..., 91	24
4	3	36, 37, 38, 39	14	92, 93, 94	25
5, 6, 7, 8	4	40	15	95, 96, ..., 99	26
9, 10	5	41, 42, ..., 50	16	100, 101, 102, 103	27
11, 12	6	51, 52, 53	17	104, 105, ..., 110	28
13	7	54, 55, 56, 57	18	111, 112, 113	29
14, 15, ..., 19	8	58, 59, ..., 62	19	114, 115, ..., 120	30
20, 21, 22, 23	9	63, 64, ..., 70	20	121	31
24, 25	10	71, 72, 73	21	122, 123	32
26, 27, 28, 29	11	74, 75, ..., 81	22		

To deduce upper bounds for $r(N)$ for larger values of N without further computation, we can simply appeal to the fact that

$$r(N + M) \le r(N) + r(M).$$

Choosing a modulus q and writing $N = aq + q_0$ with $0 \le q_0 \le k - 1$, we therefore have

$$r(N) \le ar(q) + r(q_0),$$

where we take $r(0) = 0$. It follows that, if S is any subset of S_N without three-term arithmetic progressions, then we have

$$\frac{|S|}{N} \le \frac{ar(q) + r(q_0)}{aq + q_0}. \tag{6.3}$$

PROPOSITION 6.1. *Let $N \ge 178$ be an integer and suppose that $S \subseteq S_N$ has cardinality $|S|$ satisfying $|S| > 0.27N$. Then we may conclude that S contains a nontrivial 3-term arithmetic progression. That is, there exist s_1, s_2, s_3 in S with $s_1 < s_2 < s_3$ and $s_1 + s_3 = 2s_2$.*

Proof. Suppose that $N \geq 178$ and that $S \subseteq S_N$. Suppose further that S contains no nontrivial 3-term arithmetic progressions. Applying inequality (6.3) with $q = 123$, we find that

$$\frac{|S|}{N} \leq \frac{32a + r(q_0)}{123a + q_0}, \quad \text{where } 0 \leq q_0 \leq 122. \tag{6.4}$$

Since $N \geq 178$, we see that $a \geq 1$, and checking each value $0 \leq N_0 \leq 122$ separately, we may readily verify that (6.4) implies $|S| \leq 0.27N$ unless $N \leq 533$. For the remaining values of N for which (6.4) fails to imply $|S| \leq 0.27N$, we appeal to (6.3) with either $q = 120$ or $q = 110$. We find that $|S| \leq 0.27N$ unless $q \leq 185$. To handle $182 \leq N \leq 185$, we use the partition $N = 94 + (N - 94)$, so that

$$r(N) \leq r(94) + r(91) = 49 < 0.27N \quad \text{for } 182 \leq N \leq 185.$$

Finally, for $178 \leq N \leq 181$, we write $N = 91 + (N - 91)$, whereby

$$r(N) \leq r(91) + r(90) = 48 < 0.27N \quad \text{for } 178 \leq N \leq 181. \ \blacksquare$$

Applying this result shows that, for $k \leq 15177$, there necessarily exists a 3-term arithmetic progression $\{i, i+j, i+2j\}$ of indices in $\{0, 1, \ldots, k-1\}$ such that (6.1) holds. From Proposition 2.2 and the assumption that $\log \ell > 5^k$, there thus exists an elliptic curve $E/\mathbb{Q}$ with full rational 2-torsion, without complex multiplication and with good reduction outside

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53\}. \tag{6.5}$$

In recent work of von Känel and Matschke [12], one finds the complete solution to the equation $a + b = c$ in S-units a, b and c (i.e. integers a, b and c with all their prime factors in S) for S as in (6.5). There are 1663449 triples of such solutions with $0 < a \leq b < c$, each corresponding to an elliptic curve with model

$$E_{a,b} : \ y^2 = x(x - a)(x + b). \tag{6.6}$$

Such a curve has full rational 2-torsion and good reduction outside S. Conversely, any elliptic curve over $\mathbb{Q}$ with full rational 2-torsion and good reduction outside S is isomorphic to a model (which need not be minimal) of the shape (6.6), for integers a and b such that a, b and $a + b$ are all S-units. It follows that the E whose existence is guaranteed by Proposition 2.2 is necessarily a quadratic twist of $E_{a,b}$ for one of the 1663449 possibilities found in [12].

It remains then to check, for each $83 \leq k \leq 15177$, whether we ever have, say,

$$a_p(E_{a,b}) = \pm a_p(E_0) \quad \text{for every prime } p \text{ with } k/3 < p \leq k. \tag{6.7}$$

By way of example, if $k = 83$, then we may restrict our attention to $E_{a,b}$ with good reduction outside $P_{23} = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$. The

only $E_{a,b}$ we find with good reduction outside P_{23} and $a_p(E_{a,b}) = 0$ for $p \in \{59, 67, 71, 79, 83\}$ are quadratic twists of the following curves:

Curve	Conductor	a	b
E_0	2^5	-1	0
E_1	$2^3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$	498	-408595

In the first case, the corresponding twists necessarily have complex multiplication. In the second, we have $a_{61}(E_1) = -6$, while $a_{61}(E_0) = -10$.

For each value of k in question, it is a short computation to verify that the only $E_{a,b}$ satisfying (6.7) themselves have complex multiplication (and hence cannot be isogenous to E).

It follows, therefore, that $\log \ell < 5^k$ for each $83 \leq k \leq 15177$. Since a result of Darmon and Granville [6] implies that the number of nontrivial solutions to (1.1) is finite for each fixed pair (k, ℓ) with $k + \ell \geq 6$, this completes the proof of Theorem 1.1.

7. Concluding remarks. From the proof of Theorem 1.1, it is straightforward to obtain results for the more general equation

$$n(n+d)\cdots(n+(k-1)d) = by^\ell,$$

where b is an integer whose greatest prime factor $P(b)$ is restricted in some fashion. We will omit the details here.

Acknowledgements. This research was supported in part by a grant from NSERC.

References

[1] M. A. Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. 92 (2006), 273–306.

[2] M. A. Bennett and S. Siksek, *A conjecture of Erdős, supersingular primes and short character sums*, submitted for publication.

[3] M. A. Bennett and C. M. 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* $(p, p, 3)$, Compos. Math. 140 (2004), 1399–1416.

[5] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997.

[6] H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995), 513–543.

[7] J. Dybizbański, *Sequences containing no* 3*-term arithmetic progressions*, Electron. J. Combin. 19 (2012), Paper 15, 5 pp.

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

[9] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, in: Number Theory and Its Applications, S. Kanemitsu and K. Győry (eds.), Kluwer, 1999, 145–156.
[10] K. Győry, L. Hajdu and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compos. Math. 145 (2009), 845–864.
[11] K. Győry, L. Hajdu and N. Saradha, *On the diophantine equation* $n(n+d)\cdots(n+(k-1)d) = by^l$, Canad. Math. Bull. 47 (2004), 373–388.
[12] R. von Känel and B. Matschke, *Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture*, arXiv: 1605.06079 (2016).
[13] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. 49 (1997), 1139–1161.
[14] S. Laishram and T. N. Shorey, *Perfect powers in arithmetic progressions*, J. Combin. Number Theory 7 (2016), 95–110.
[15] R. Marszałek, *On the product of consecutive elements of an arithmetic progression*, Monatsh. Math. 100 (1985), 215–222.
[16] 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.
[17] T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.
[18] N. Saradha, *Applications of the explicit abc-conjecture to two Diophantine equations*, Acta Arith. 151 (2012), 401–419.
[19] N. Saradha and T. N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. 99 (2001), 363–388.
[20] N. Saradha and T. N. Shorey, *Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression*, Compos. Math. 141 (2005), 541–560.
[21] L. Schoenfeld, *Sharper bounds for the Chebyshev functions* $\theta(x)$ *and* $\psi(x)$ *II*, Math. Comp. 30 (1976), 337–360.
[22] T. N. Shorey, *Some exponential Diophantine equations*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge Univ. Press, 1988, 352–365.
[23] T. N. Shorey, *Exponential diophantine equations involving products of consecutive integers and related equations*, in: Number Theory, R. P. Bambah et al. (eds.), Hindustan Book Agency, 2000, 463–495.
[24] T. N. Shorey, *Powers in arithmetic progressions (II)*, RIMS Kokyuroku 1274 (2002), 202–214.
[25] T. N. Shorey, *Diophantine approximations, Diophantine equations, transcendence and applications*, Indian J. Pure Appl. Math. 37 (2006), 9–39.
[26] T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression*, in: A Tribute to Paul Erdős (A. Baker et al., eds.), Cambridge Univ. Press, 1990, 385–389.
[27] T. N. Shorey and R. Tijdeman, *Perfect powers in products of terms in an arithmetical progression*, Compos. Math. 75 (1990), 307–344.
[28] R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications, Kluwer, 1989, 215–243.

Michael A. Bennett
Department of Mathematics
University of British Columbia
Vancouver, BC, Canada V6T 1Z2
E-mail: bennett@math.ubc.ca