Compositio Math. 141 (2005) 541–560
DOI: 10.1112/S0010437X04001125

Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression

N. Saradha and T. N. Shorey

Abstract

Let $n, d, k \geqslant 2, b, y$ and $\ell \geqslant 3$ be positive integers with the greatest prime factor of b not exceeding k. It is proved that the equation $n(n+d)\cdots(n+(k-1)d) = by^\ell$ has no solution if d exceeds d_1, where d_1 equals 30 if $\ell = 3$; 950 if $\ell = 4$; 5×10^4 if $\ell = 5$ or 6; 10^8 if $\ell = 7$, 8, 9 or 10; 10^{15} if $\ell \geqslant 11$. This confirms a conjecture of Erdős on the above equation for a large number of values of d.

1. Introduction

For an integer $\nu > 1$, we define $P(\nu)$ to be the greatest prime factor of ν and we write $P(1) = 1$. In this paper, we consider the equation

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

in positive integers n, d, k, b, y and ℓ, where $d \geqslant 1$, $k \geqslant 2$, $\ell \geqslant 2$, $P(b) \leqslant k$, $\gcd(n, d) = 1$ and b is ℓ-free. We observe that (1.1) has infinitely many solutions if $k = 2$. Therefore, we always suppose that $k \geqslant 3$. Furthermore, Erdős and Selfridge [ES75] have completely solved (1.1) with $d = 1$ for $P(b) < k$, Saradha [Sar97] has completely solved (1.1) for $P(b) = k$ with $k \geqslant 4$ and Győry [Győ98] has completely solved (1.1) for $P(b) = k$ with $k = 3$, $\ell > 2$. In the case $k = 3$, $\ell = 2$ the only solutions of (1.1) are given by $n = 1, 2, 48$ as a consequence of some old Diophantine results, see [Sar98] for a history.

From now onwards we assume that $d > 1$. Then we always suppose that $(n, d, k) \neq (2, 7, 3)$ so that $P(\Delta) > k$ by a result of Shorey and Tijdeman [ST90]. Erdős conjectured that (1.1) implies that k is bounded by an absolute constant. Shorey [Sho00] showed that the above conjecture for $\ell \geqslant 4$ is a consequence of the *abc*-conjecture. A stronger conjecture states the following.

Conjecture 1. Equation (1.1) implies that $(k, \ell) = (3, 3)$, $(4, 2)$ or $(3, 2)$.

On the other hand, it is known that (1.1) has infinitely many solutions if $(k, \ell) = (3, 3)$, $(4, 2)$ or $(3, 2)$, see Tijdeman [Tij89]. It was conjectured by Tijdeman that the number of triples (n, d, k) satisfying (1.1) with $k > 2$, $\ell > 1$, $k + \ell > 6$ is finite. Let $b = 1$. Then Darmon and Granville [DG95] conjectured that (1.1) implies that $(k, \ell) = (3, 2)$, in which case we get parametric solutions given by $(n, d) \in \{((t^2+2tu-u^2)^2, 4tu(u^2-t^2)), (2(t^2-u^2)^2, 6t^2u^2-t^4-u^4)\}$ with $\gcd(t, u) = 1$ and $t+u$ odd. The cases $(k, \ell) = (3, 3), (4, 2)$ are impossible by an old result of Euler, see [DG95]. When d is fixed, Marszalek [Mar85] confirmed Erdős conjecture. When $\ell = 2$, it has been proved that $d \geqslant 23$, $d \geqslant 31$ and $d \geqslant 105$ in Saradha [Sar98], Filakovszky and Hajdu [FH01] and Saradha and Shorey [SS03], respectively. From now onwards we assume that $\ell \geqslant 3$. Saradha [Sar97] showed that $d \geqslant 7$ unless $d = 5$, $k = 3$. Furthermore, Saradha and Shorey [SS01] showed that (1.1) with $k \geqslant 4$ does

Received 15 July 2003, accepted in final form 14 April 2004, published online 21 April 2005.
2000 Mathematics Subject Classification Primary 11D61.
Keywords: arithmetic progressions, Diophantine equations, elliptic equations.

not hold if d is of the form $2^a 3^b 5^c$, where a, b, c are non-negative integers. Let d_1 be given by

$$d_1 = \begin{cases} 30 \text{ if } \ell = 3; \\ 950 \text{ if } \ell = 4; \\ 5 \times 10^4 \text{ if } \ell = 5, 6; \\ 10^8 \text{ if } \ell = 7, 8, 9, 10; \\ 10^{15} \text{ if } \ell \geqslant 11. \end{cases} \tag{1.2}$$

We prove the following theorem.

Theorem 1. *Assume (1.1) and $k \geqslant 4$ if $\ell > 3$. Then $d > d_1$.*

We have not been able to prove Theorem 1 for $k = 3$ whenever $\ell > 3$. From now onwards, we suppose that $k \geqslant 4$ whenever $\ell > 3$. Theorem 1 confirms Conjecture 1 for a large number of values of d. For a survey of results on (1.1), we refer the reader to Shorey [Sho00, Sho02a, Sho02b]. We now give a plan of the proof of Theorem 1. We assume (1.1) with $d \leqslant d_1$. Furthermore, by Lemma 1, there is no loss of generality in assuming that the following hypothesis holds.

Hypothesis A. We have $d \leqslant d_1$ and either k is prime or $k = 4$ if $\ell > 3$.

The proof depends on giving a good lower bound for

$$\delta = \frac{n + (k-1)d}{k^{l+1}}, \tag{1.3}$$

say $\delta > \delta_1$. We achieve this by means of an iterative procedure in Lemma 3. On the other hand, we obtain an upper bound

$$\delta < \delta_2 \tag{1.4}$$

by Lemmas 6 and 12. Furthermore, we compare the lower and upper bounds of δ in Lemma 13 to bound ℓ and k. Let ℓ and k be fixed. By (1.3) and (1.4), we have

$$\delta_1 k^{\ell+1} < n + (k-1)d < \delta_2 k^{\ell+1}. \tag{1.5}$$

Let $\ell > 3$. Then we use Algorithm 1 (see § 8) to see that (1.1) is not satisfied for all values of n given by (1.5). For $\ell = 3$, we use Algorithm 2 (see § 10). The iterative procedure referred above has its origin in [SS01, Lemma 3] and [SS03, Lemma 6]. Algorithm 2 is a refinement and an extension of the algorithm given in [SS01]. Algorithm 1 is a new contribution in this paper. Algorithms 1 and 2 provide a method for solving (1.1) whenever the variables n, d, k, ℓ are bounded. The bound d_1 we have given in Theorem 1 is not optimal. Increasing the value of d_1 would result in heavier computation. All of our computations are carried out with MATHEMATICA and we use SIMATH for solving certain elliptic equations in integers.

2. Notation and preliminaries

Let $q_1 < q_2 < \cdots$ be the sequence of all primes coprime to d and let $p_1 < p_2 < \cdots$ be the sequence of all primes. We write $\pi_d(x)$ for the number of primes $\leqslant x$ and coprime to $d, \pi(x)$ for the number of primes $\leqslant x$. We use the estimates

$$q_i \geqslant p_i \geqslant i \log i \quad \text{for } i \geqslant 1; \quad \pi_d(x) \leqslant \pi(x) \leqslant \frac{x}{\log x} + \frac{1.5x}{\log^2 x} \quad \text{for } x \geqslant 1; \quad \pi(x) > \frac{x}{\log x} \quad \text{for } x > 17. \tag{2.1}$$

See [RS62, p. 69] for the above inequalities. For an integer $x > 0$, we write $q_i(x) = q_{\pi_d(x)+i}$ with $i \geqslant 1$. We set $\beta = \beta(d,k) = \prod_{p|d} p^{-\mathrm{ord}_p(k-1)!}$ and

$$\beta_1 = \beta_1(d,k) = (k-1)!\beta. \tag{2.2}$$

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

For $s > 0$ and $h \geqslant 0$, we define

$$\beta_2(s,h) = \beta_2(d,k,\ell,s,h) = k - \frac{(k-1)\,\log(k-1) + \log\beta}{\ell\,\log(k-1) + \log s - \log 2} - \pi_d(k) - h, \tag{2.3}$$

$$\beta_3(s,h) = \max\,(1, [\beta_2(s,h)] + 1), \tag{2.4}$$

$$\beta_4(s,h) = \beta_4(d,k,\ell,s,h) = k - \frac{(k-1)\,\log(k-1) + \log\beta}{(\ell+1)\,\log(k-1) + \log s - \log 2} - \pi_d(k) - h \tag{2.5}$$

and

$$\beta_5(s,h) = \max(1, [\beta_4(s,h)] + 1). \tag{2.6}$$

Since the left-hand side of (1.1) is divisible by a prime exceeding k and $P(b) \leqslant k$, we have $n+(k-1)d > k^\ell$. For $k \geqslant 4$, we see from [SS01, Theorem 4′] and [SST02, Theorem 1] that Δ is divisible by at least $\chi_0 = [\frac{1}{5}\pi(k)] + 2$ primes exceeding k, except when (n,d,k) equals one of the tuples $(1,5,4)$, $(2,7,4)$, $(3,5,4)$, $(1,2,5)$, $(2,7,5)$, $(4,7,5)$, $(4,23,5)$. We check that these values of (n,d,k) do not satisfy (1.1). Thus, for $k \geqslant 4$ we conclude that Δ is always divisible by at least χ_0 primes $> k$. Therefore, we see from (1.1) that

$$n + (k-1)d \geqslant q^\ell_{\chi_0}(k) \quad \text{for } k \geqslant 4. \tag{2.7}$$

Hence, from (1.3), we get $\delta > 1/k$. Furthermore, we derive from (1.1) that

$$n + id = a_i x_i^\ell, \quad P(a_i) \leqslant k, \quad a_i \text{ is } \ell\text{th power free for } 0 \leqslant i < k \tag{2.8}$$

and

$$n + id = A_i X_i^\ell, \quad P(A_i) \leqslant k, \quad \gcd\biggl(\prod p, X_i\biggr) = 1 \quad \text{for } 0 \leqslant i < k \tag{2.9}$$

where the product $\prod p$ is taken over all primes p with $p \leqslant k$.

We say that an integer $N \geqslant 1$ has *Property* P_0 if all the prime factors of N which are greater than k divide it to an order $\equiv 0 \pmod{\ell}$. From (2.8) and (2.9), we see that every term of Δ has Property P_0. Suppose that N_1 and N_2 are integers satisfying $0 < N_1 < N_2$. Let $r \geqslant 1$ and t be integers. We set

$$M_{r,t} = M_{r,t}(N_1, N_2) = N_1\left(1 - \frac{t}{r}\right) + N_2\frac{t}{r}. \tag{2.10}$$

We say that the triple (N_1, N_2, r) has *Property* P_1 if (i) or (ii) given below holds according as $r > 1$ or $r = 1$, respectively.

(i) Let $r > 1$. Then $(N_2 - N_1)/r$ is an integer and $M_{r,t}$ has Property P_0 for every t with $0 \leqslant t \leqslant r$.

(ii) Let $r = 1$. Then either $M_{1,t}$ with $0 \leqslant t \leqslant [\frac{k}{2}]$ has Property P_0 or $M_{1,t}$ with $-[\frac{k}{2}] \leqslant t \leqslant 0$ has Property P_0.

Suppose that $N_1 = n + id$, $N_2 = n + jd$ with $0 \leqslant i < j < k$, then $(N_2 - N_1)/(j-i) = d$ and $M_{j-i,t}$ with $0 \leqslant t \leqslant j-i$ is a term of the product Δ and hence has Property P_0. Therefore (i) is satisfied. Similarly (ii) is also satisfied. Thus, the triple $(N_1, N_2, j-i)$ has Property P_1. We say that the triple (N_1, N_2, r) has *Property* P_2 if $(N_2 - N_1)/r$ is an integer and is divisible by a prime $\equiv 1 \pmod{\ell'}$ for every odd prime ℓ' dividing ℓ. By Lemma 9, we see that if $k \geqslant 4$ and $N_1 = n + id$, $N_2 = n + jd$ with $0 \leqslant i < j < k$, then the triple $(N_1, N_2, j-i)$ has Property P_2.

Let $S = \{A_0, \ldots, A_{k-1}\}$ and $T = \{a_0, \ldots, a_{k-1}\}$. Furthermore, let $I = \{\mu \mid X_\mu \neq 1$ with $0 \leqslant \mu < k\}$ and let S_1 be the set of $A_\mu \in S$ with $\mu \in I$. As already mentioned, we assume that $|I| \geqslant 1$. Suppose that $m_1 \geqslant 1$ and $m_2 \geqslant 0$ are integers such that $m_1 + m_2 \leqslant \pi(k)$. Now we state some counting functions, which were first introduced in Erdős and Selfridge [ES75, pp. 297–299] for the case of consecutive integers. Let $H(d,k,m_1,m_2)$ denote the number of distinct a_i in T that are composed only of $q_1, \ldots, q_{m_1}$ and divisible by at most one of the primes $q_{m_1+1}, \ldots, q_{m_1+m_2}$

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

that divides at most to the first power. In particular, when $m_2 = 0$, we see that $H(d, k, m_1, 0)$ denotes the number of distinct a_i in T that are composed only of $q_1, \ldots, q_{m_1}$. It can be seen that

$$H(d, k, m_1, m_2) \geqslant |T| - \sum_{i=m_1+m_2+1}^{\pi(k)} \left(\left[\frac{k}{q_i}\right] + \epsilon'_i \right) - \sum_{m_1+1 \leqslant j \leqslant h \leqslant m_1+m_2} \left(\left[\frac{k}{q_j q_h}\right] + \epsilon'_{jh} \right) \tag{2.11}$$

where $\epsilon'_i = 0$ if $q_i \mid k$ or $q_i > k$, $\epsilon'_i = 1$ otherwise and $\epsilon'_{jh} = 1$ if $q_j q_h \nmid k$ and $q_j, q_h \leqslant k$, $\epsilon'_{jh} = 0$ otherwise. We define $\epsilon_i = 0$ if $p_i \mid k$ and $\epsilon_i = 1$ otherwise; $\epsilon_{jh} = 0$ if $p_j p_h | k$ and $\epsilon_{jh} = 1$ otherwise. Then we find that

$$\left[\frac{k}{q_i}\right] + \epsilon'_i \leqslant \left[\frac{k}{p_i}\right] + \epsilon_i \quad \text{and} \quad \left[\frac{k}{q_j q_h}\right] + \epsilon'_{jh} \leqslant \left[\frac{k}{p_j p_h}\right] + \epsilon_{jh}.$$

For showing the first inequality, we may assume that $\epsilon'_i = 1$, $\epsilon_i = 0$ implying that $q_i > p_i, p_i | k$ and the assertion follows. The proof for the second inequality is similar. Hence we get from (2.11) that

$$H(d, k, m_1, m_2) \geqslant H'_0(k, m_1, m_2) \tag{2.12}$$

where

$$H'_0(k, m_1, m_2) = |T| - \sum_{i=m_1+m_2+1}^{\pi(k)} \left(\left[\frac{k}{p_i}\right] + \epsilon_i \right) - \sum_{m_1+1 \leqslant j \leqslant h \leqslant m_1+m_2} \left(\left[\frac{k}{p_j p_h}\right] + \epsilon_{jh} \right). \tag{2.13}$$

In particular, we have

$$H(d, k, m_1, 0) \geqslant H'_0(k, m_1, 0) = |T| - \sum_{i=m_1+1}^{\pi(k)} \left(\left[\frac{k}{p_i}\right] + \epsilon_i \right). \tag{2.14}$$

We use the above inequality for $k \leqslant 2957$. If $k > 2957$, we use $H(d, k, m_1, m_2)$ and $H'_0(k, m_1, m_2)$ with $m_2 > 0$. When $m_2 > 0$, we take m_1 and m_2 such that $p_1 < \cdots < p_{m_1} \leqslant k^{3/10} < p_{m_1+1} < \cdots < p_{m_1+m_2} \leqslant \sqrt{k}$. From (2.13) we then derive that

$$H'_0(k, m_1, m_2) \geqslant H''_0(k, m_1, m_2) \tag{2.15}$$

where

$$H''_0(k, m_1, m_2) := |T| - \sum_{\sqrt{k} < p \leqslant k} \left(\left[\frac{k}{p}\right] + 1 \right) - \frac{k}{2} \left(\sum_{i=1}^{m_2} \frac{1}{p^2_{m_1+i}} + \left(\sum_{i=1}^{m_2} \frac{1}{p_{m_1+i}} \right)^2 \right) - \binom{m_2+1}{2}. \tag{2.16}$$

By combining (2.12) and (2.15), we get

$$H(d, k, m_1, m_2) \geqslant H''_0(k, m_1, m_2). \tag{2.17}$$

Let $|T| = k$, i.e. all a_i are distinct. In Table 1, we display a lower bound $H_1(m_1)$ for $H'_0(k, m_1, 0)$ given by (2.14) when k varies over an interval and m_1 is suitably chosen. In Table 2, we display a lower bound $H_2(m_1, m_2)$ for $H''_0(k, m_1, m_2)$ given by (2.16) when k varies over an interval and m_1, m_2 are suitably chosen.

By Table 1 and (2.14), we have $H(d, k, m_1, 0) \geqslant 4$ for $k = 23, 24$. We sharpen this as $H(d, k, m_1, 0) \geqslant 5$ for $k = 23, 24$. Let $k = 24$. Suppose that $H(d, k, m_1, 0) = 4$. This means that the number of a_i that the primes $23, 19, 17, 13, 11, 7, 5$ divide is given by $2, 2, 2, 2, 3, 4, 5$, respectively, and no two primes divide the same a_i. This implies that 23 divides a_0, a_{23}. Then it is impossible that 11 divides three different a_i. The argument for $k = 23$ is similar. For $m_1 > 0$ and $\alpha_i > 0$ with $1 \leqslant i \leqslant m_1$, we also need the following counting function. Let $G(d, k, m_1, \alpha_1, \ldots, \alpha_{m_1})$ denote the number of A_j in S that are composed of $q_1, \ldots, q_{m_1}$ and $\text{ord}_{q_i}(A_j) \leqslant \alpha_i - 1$ for $1 \leqslant i \leqslant m_1$.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

Table 1.

m_1	Range of k	$H_1\ (m_1)$	m_1	Range of k	$H_1\ (m_1)$
2	$4 \leqslant k \leqslant 10$	4	5	$286 \leqslant k \leqslant 600$	27
2	$11 \leqslant k \leqslant 22$	5	6	$601 \leqslant k \leqslant 1097$	45
2	23, 24	4	7	$1098 \leqslant k \leqslant 1669$	77
3	$25 \leqslant k \leqslant 90$	10	8	$1670 \leqslant k \leqslant 2478$	132
4	$91 \leqslant k \leqslant 285$	16	9	$2479 \leqslant k \leqslant 2957$	227

Table 2.

m_1	m_2	Range of k	$H_2\ (m_1, m_2)$	m_1	m_2	Range of k	$H_2\ (m_1, m_2)$
4	12	2958–2960	271	6	15	5329–6240	832
5	11	2961–3480	420	6	16	6241–6888	917
5	12	3481–3720	465	6	17	6889–7920	986
5	13	3721–4488	494	6	18	7921–9408	1071
5	14	4489–5040	545	6	19	9409–10 200	1171
5	15	5041–5165	582	6	20	10 201–10 608	1237
6	14	5166–5328	792	6	21	10 609–11 379	1285

Then $G(d, k, m_1, \alpha_1, \ldots, \alpha_{m_1}) \geqslant G_0(k, m_1, \alpha_1, \ldots, \alpha_{m_1})$ where

$$G_0 = G_0(k, m_1, \alpha_1, \ldots, \alpha_{m_1}) = |S| - \sum_{i=1}^{m_1} \left(\left[\frac{k}{p_i^{\alpha_i}} \right] + \epsilon_i'' \right) - \sum_{i=m_1+1}^{\pi(k)} \left(\left[\frac{k}{p_i} \right] + \epsilon_i \right) \tag{2.18}$$

with ϵ_i as defined earlier and $\epsilon_i'' = 0$ if $p_i^{\alpha_i} \mid k, \epsilon_i'' = 1$ otherwise.

We conclude this section with a lemma which is useful for computation.

Lemma 1. *Suppose that k_1 and k_2 are two consecutive primes and let k' be an integer with $k_1 < k' < k_2$. Suppose that (1.1) does not hold for $k = k_1$. Then (1.1) does not hold for $k = k'$.*

Proof. Suppose that (1.1) holds for $k = k'$. Since $k_1 < k' < k_2$ and k_1, k_2 are consecutive primes, $P(b) \leqslant k'$ implies that $P(b) \leqslant k_1$. Let $k' = k_1 + h$. By deleting the terms $n+(k'-1)d, \ldots, n+(k'-h)d$, we see from (2.8) that

$$n(n+d)\cdots(n+(k_1-1)d) = b' y_1^\ell, \quad P(b') \leqslant k_1$$

for some positive integers b' and y_1. Thus (1.1) holds with $k = k_1$, a contradiction. □

For the proof of Theorem 1, we see from Lemma 1 that it suffices to show that (1.1) does not hold under Hypothesis A.

3. An iterative procedure to improve the lower bound for $n + (k-1)d$

In this section, we give an iterative procedure in Lemma 3 by which we improve the lower bound for $n+(k-1)d$ given by (2.7) and [SS01, Lemma 3]. This procedure is an analogue of that given for the case $\ell = 2$ in [SS03]. We first give a lemma in which we estimate the number of elements of I.

Lemma 2. *Let $k \geqslant 4$. Then (1.1) implies that*

$$|I| > k - \frac{(k-1)\,\log(k-1) + \log\beta}{\log d + \log(k-1)} - \pi_d(k) - 1 \tag{3.1}$$

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

and

$$|I| > k - \frac{(k-1)\log(k-1) + \log\beta}{\log n_0} - \pi_d(k) - \phi \tag{3.2}$$

where $n_0 = \max(n, 3)$, $\phi = 1$ *if* $n = 1, 2$ *and* $\phi = 0$ *if* $n > 2$.

The proof is similar to [SS03, Lemma 3]. We require $\pi_d(k)$ instead of $\pi_d(k-1)$ in [SS03, Lemma 3] since we now have $P(A_i) \leqslant k$. In the next lemma, we describe the iterative procedure.

Lemma 3. *Assume (1.1) such that all* A_j *given by (2.9) are distinct. Then the following assertions hold.*

(i) *We have*

$$n + (k-1)d \geqslant \max(\beta_3(1,\eta_1)p^{\ell}_{\pi(k)+1}, p^{\ell}_{\pi(k)+\beta_3(1,\eta_1)})$$

where $\eta_1 = 0$ *if* $d < k^{\ell-1}/2$ *and* $\eta_1 = 1$ *otherwise.*

(ii) *Let* $n + (k-1)d \geqslant G_1 k^{\ell+1}$ *with* $G_1 \geqslant 1/k$. *For* $i \geqslant 2$, *define*

$$g_i k^{\ell+1} \leqslant \beta_5(G_{i-1}, \eta_i)p^{\ell}_{\pi(k)+1}, \quad G_i = \max(G_{i-1}, g_i)$$

where $\eta_i = 0$ *if* $d < G_{i-1}k^{\ell}/2$ *and* $\eta_i = 1$ *otherwise. Then* $n + (k-1)d \geqslant G_i k^{\ell+1}$.

(iii) *Let* i_0 *be fixed with* $n + (k-1)d \geqslant G_{i_0}k^{\ell+1}$ *and* $\eta_{i_0+1} = \eta'_1$. *Let*

$$h_1 = \frac{\beta_5(G_{i_0}, \eta_{i_0+1})}{k}, \quad h'' < h_1, v_1 \leqslant \frac{([h''k]+1)p^{\ell}_{h_1k-[h''k]+\pi(k)}}{k^{\ell+1}}.$$

Then $n + (k-1)d \geqslant V_1 k^{\ell+1}$ *where* $V_1 = \max(G_{i_0}, v_1)$.

(iv) *For* $i \geqslant 2$, *we define*

$$v_i \leqslant \frac{([h''k]+1)p^{\ell}_{h_ik-[h''k]+\pi(k)}}{k^{\ell+1}}, \quad V_i = \max(V_{i-1}, v_i)$$

where

$$h_i = \frac{\beta_5(V_{i-1}, \eta'_i)}{k} \quad \text{with } \eta'_i = \begin{cases} 0 & \text{if } d < V_{i-1}k^{\ell}/2 \\ 1 & \text{otherwise.} \end{cases}$$

Then $n + (k-1)d \geqslant V_i k^{\ell+1}$.

Proof. (i) Suppose that $d \geqslant k^{\ell-1}/2$. Then we use (3.1) to estimate $|I|$. If $d < k^{\ell-1}/2$, then we use (2.7) to find $n > k^{\ell}/2$, which we use in (3.2) to estimate $|I|$. Thus we get $|I| > \beta_2(1,\eta_1)$, which, together with $|I| \geqslant 1$, implies that $|I| \geqslant \beta_3(1,\eta_1)$. We arrange all the X_j with $j \in I$ in increasing order. Since these X_j are all distinct, we have $n + (k-1)d \geqslant p^{\ell}_{\pi(k)+\beta_3(1,\eta_1)}$. Since A_j are distinct, we have $|S_1| = |I| \geqslant \beta_3(1,\eta_1)$. Now we arrange these A_j in S_1 in increasing order and observe that each of the corresponding X_j has a prime factor greater than k. This gives $n + (k-1)d \geqslant \beta_3(1,\eta_1)p^{\ell}_{\pi(k)+1}$, which proves (i).

(ii) Let $n + (k-1)d \geqslant G_1k^{\ell+1}$. Note that $n + (k-1)d \geqslant G_1k^{\ell+1}$ with $G_1 = 1/k$ is satisfied by (2.7). We prove the assertion for $i = 2$. We use (3.1) if $d \geqslant G_1k^{\ell}/2$ and if otherwise, we see that $n \geqslant G_1k^{\ell+1}/2$ and we use (3.2) to estimate $|I|$. Hence $|S_1| = |I| \geqslant \beta_5(G_1, \eta_2)$, which implies that $n + (k-1)d \geqslant g_2k^{\ell+1}$. Thus $n + (k-1)d \geqslant G_2k^{\ell+1}$. The assertion for $i \geqslant 3$ follows similarly.

(iii) Let $n + (k-1)d \geqslant G_{i_0}k^{\ell+1}$. We proceed as in (ii) to get $|S_1| \geqslant \beta_5(G_{i_0}, \eta_{i_0+1})$. Thus there are at least h_1k distinct A_j with $j \in I$. We arrange them in increasing order and remove the first $[h''k]$ of these A_j. Thus we are left with $h_1k - [h''k] \geqslant 1$ of the A_j each of which exceeds $[h''k]+1$ and the largest X_j is divisible by a prime greater than or equal to $p_{h_1k-[h''k]+\pi(k)}$. Now the assertion follows immediately.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

(iv) We have $n+(k-1)d \geqslant V_1 k^{\ell+1}$ by (iii). Hence we get $|S_1| \geqslant \beta_5(V_1, \eta_2')$. Thus there are at least $h_2 k$ distinct A_j with $j \in I$. Furthermore, $\beta_5(s,h)$ is a non-decreasing function of s. Hence $h_2 \geqslant h_1$. Now we proceed as in (iii) to get $n+(k-1)d \geqslant ([h''k]+1)p^{\ell}_{h_2 k-[h''k]+\pi(k)}$. Hence $n+(k-1)d \geqslant \max(V_1, v_2)k^{\ell+1}$. This proves the assertion for $i=2$. The assertion for $i \geqslant 3$ follows similarly. □

We illustrate Lemma 3 by means of an example. In this example and at all places in the paper where we compute δ, we take $h''=0.16$ and we iterate four times. The value of h'' is not optimal for every k. Furthermore, in this example, we apply Lemma 3 with $d \leqslant k^{\ell-1}/2$ so that $\eta_i = \eta_i' = 0$ for $1 \leqslant i \leqslant 4$.

Example. We show that

$$\delta \geqslant 6.0048 k^{\ell+1} \quad \text{for } k \geqslant 173 \text{ and } \ell \geqslant 3. \tag{3.3}$$

We observe that the functions β_3 and β_5 given by (2.4) and (2.6) are non-decreasing functions of ℓ and k. Hence, while evaluating these functions in this example, it is enough to evaluate them at $k=173$ and $\ell=3$. We first take $k=173$. By using exact values of $\pi(k)$, we find that $\beta_3(1,0) \geqslant 73$. Now using exact values for p_i, by Lemma 3(i) we get $n+(k-1)d \geqslant \max(73 \times 179^{\ell}, 617^{\ell}) \geqslant 0.4674\ k^{\ell+1}$. In Lemma 3(ii), we take $G_1 = 0.4674$. We compute $g_2 = 0.5570$. Thus $G_2 = 0.5570$. Similarly we find $G_3 = G_4 = 0.5634$. In Lemma 3(iii), we take $i_0 = 4$. We get $h_1 > 0.5 > 0.16 = h''$. Hence $v_1 = 5.1160$. Thus $V_1 = 5.1160$. In Lemma 3(iv), we compute $v_2 = 5.8194$. Hence $V_2 = 5.8194$. Similarly we find $V_3 = V_4 = 6.0048$. Thus we obtain (3.3).

Now let $k \geqslant 3000$. In Lemma 3 we use the approximate values for p_i and $\pi(k)$ given by (2.1). We also use $p_{\pi(k)+1} > k$. Thus we find by Lemma 3(i) that $n+(k-1)d \geqslant \rho_1 k^{\ell+1}$ where

$$\rho_1 = 1 - \frac{\log(k-1)}{\ell \log(k-1) - \log 2} - \frac{1}{\log k} - \frac{1.5}{\log^2 k} - \frac{1}{k}.$$

We observe that ρ_1 increases as k and ℓ increase. We compute ρ_1 at $k=3000$ and $\ell=3$ to get $n+(k-1)d \geqslant 0.5081 k^{\ell+1}$. Thus $n+(k-1)d \geqslant 0.5081 k^{\ell+1}$ for all $k \geqslant 3000$ and $\ell \geqslant 3$. Next we apply the iterative procedure of Lemma 3(ii). We take $G_1 = \rho_1$. Then for $i \geqslant 2$, we get $n+(k-1)d \geqslant \rho_i k^{\ell+1}$ where

$$\rho_i = 1 - \frac{\log(k-1)}{(\ell+1)\log(k-1) + \log\rho_{i-1} - \log 2} - \frac{1}{\log k} - \frac{1.5}{\log^2 k} - \frac{1}{k}.$$

We observe that ρ_i is an increasing function of k and ℓ. We compute $\rho_2 = 0.5901$, $\rho_3 = \rho_4 = 0.5914$. Thus $n+(k-1)d \geqslant 0.5914 k^{\ell+1}$ for all $k \geqslant 3000$ and $\ell \geqslant 3$. Finally, we apply the iterative procedure of Lemma 3(iii), (iv). We take $G_4 = 0.5914$ and $h''=0.16$. We set $\rho_0' = 0.5914$. Then for $i \geqslant 1$ we get $n+(k-1)d \geqslant \rho_i' k^{\ell+1}$ where

$$\rho_i' = h''(h_i'-h'')^{\ell}\log^{\ell}\left(h_i'k - h''k + \frac{k}{\log k}\right)$$

with

$$h_i' = 1 - \frac{\log(k-1)}{(\ell+1)\log(k-1) + \log\rho_{i-1}' - \log 2} - \frac{1}{\log k} - \frac{1.5}{\log^2 k} - \frac{1}{k}.$$

We observe that ρ_i' is an increasing function of ℓ and $k \geqslant 200$ by noticing that $h_i' > \rho_1$ and $(h_i'-h'')\log(h_i'k - h''k + k/\log k) > 1$ for $k \geqslant 200$. We compute $h_1' = 0.5914$, $\rho_1' = 5.2507$; $h_2' = 0.6086$, $\rho_2' = 5.9770$; $h_3' = 0.609\,63$, $\rho_3' = 6.0191$, $h_4' = 0.609\,68$, $\rho_4' = 6.0213$. Thus we obtain (3.3) for $k \geqslant 3000, l \geqslant 3$. Now for k with $173 < k < 3000$, we apply Lemma 3 with exact values of p_i and $\pi(k)$ as in the case $k=173$ to obtain (3.3). This completes the proof of (3.3). □

It is clear from the example above that the lower bound given by Lemma 3 for δ is a non-decreasing function of ℓ and k. We use this fact without mentioning it in the following.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

4. Distinctness of A_j

A pre-requisite for the iterative procedure in Lemma 3 is that all A_j are distinct. In this section, we show that when A_j are not all distinct, then we can bound from above n and k in terms of ℓ and d. These bounds are decreasing functions of ℓ and $1/d$ (see (4.1)). Using these bounds we show in Corollary 1 that A_j are distinct whenever (1.1) with Hypothesis A holds.

Lemma 4. *Suppose that (1.1) holds with $k \geqslant 4$. Then either A_j with $0 \leqslant j < k$ are distinct or*

$$k \leqslant \left(\left(\frac{d}{2\ell}\right)^{\ell/(\ell-1)} + \frac{d}{k^{1/(\ell-1)}}\right)^{(\ell-1)/(\ell^2-2\ell)} \quad \text{and} \quad n < \left(\frac{kd}{2\ell}\right)^{\ell/(\ell-1)}. \tag{4.1}$$

Proof. Suppose that there exist A_i, A_j with $0 \leqslant j < i < k$ such that

$$A_i = A_j. \tag{4.2}$$

Then we see from (2.9) that $X_i \geqslant X_j + 2$ and

$$(k-1)d \geqslant (i-j)d = (n+id) - (n+jd) = A_i X_i^\ell - A_j X_j^\ell \geqslant 2\ell A_j X_j^{\ell-1}. \tag{4.3}$$

Thus it follows that $kd > 2\ell(A_j X_j^\ell)^{(\ell-1)/\ell} \geqslant 2\ell n^{(\ell-1)/\ell}$. This gives the bound for n in (4.1). Furthermore, we use (2.7) to get

$$k^\ell < q_{\chi_0}^\ell(k) \leqslant n + (k-1)d < \left(\frac{kd}{2\ell}\right)^{\ell/(\ell-1)} + kd, \tag{4.4}$$

which gives the estimate for k in (4.1). □

As a consequence of Lemma 4, we get the following.

Lemma 5. *Assume (1.1) with Hypothesis A and $k \geqslant 4$. Suppose that A_j are all not distinct. Then*

$$\begin{cases} \ell = 4, k = 4; \quad \ell = 5, k \leqslant 7; \quad \ell = 6, k = 4; \quad \ell = 7, k \leqslant 11; \quad \ell = 8, k \leqslant 7; \quad \ell = 9, 10, k = 4; \\ \ell = 11, k \leqslant 19; \quad \ell = 12, k \leqslant 13; \quad \ell = 13, 14, k \leqslant 7; \quad \ell = 15, k \leqslant 5; \quad \ell = 16, 17, 18, k = 4. \end{cases} \tag{4.5}$$

Proof. Assume (1.1) with Hypothesis A and $k \geqslant 4$. Suppose that A_j are not all distinct. Then (4.1) and (4.4) are valid. By (4.1), we see that $k \leqslant 5$ for $\ell \geqslant 19$, which we sharpen by (4.4) to $k < 4$ for $\ell \geqslant 19$. Therefore $\ell \leqslant 18$. Let $\ell = 4$. Then $d \leqslant d_1 = 950$. We use (4.1) to get $k \leqslant 13$. Now for $5 \leqslant k \leqslant 13$, we find that (4.4) is not valid. Thus $k = 4$. The bound for k in (4.5) for all other values of $\ell \leqslant 18$ is found in a similar manner. □

Now we proceed to exclude all of the values of ℓ and k in (4.5). We show the following.

Corollary 1. *Assume (1.1) with Hypothesis A and $k \geqslant 4$. Then A_j are distinct.*

Proof. Assume (1.1) with Hypothesis A and $k \geqslant 4$. Suppose that A_j are not all distinct. Then (4.1)–(4.5) are valid. We fix k, ℓ where k, ℓ are given by (4.5). From (4.4), we see that $n + (k-1)d < \delta_3$ where δ_3 is a bounded positive number. Let $1 \leqslant r < k$. We take $U_1(r)$ to be the set of divisors of r. Let U_2 be the set of all positive integers not exceeding $\delta_3^{1/\ell}$ and having the least prime factor greater than k. We always include 1 in U_2. We form $U_3(r)$ to be the set of pairs (hX^ℓ, hY^ℓ) with $h \in U_1(r)$ and X, Y in U_2 with $X < Y$ and $\gcd(X, Y) = 1$. Let U_4 be the set of triples (hX^ℓ, hY^ℓ, r) with $(hX^\ell, hY^\ell) \in U_3(r)$, $1 \leqslant r < k$ such that the triple (hX^ℓ, hY^ℓ, r) has Property P_1. From (4.2)–(4.4), we find that there exist $0 \leqslant j < i < k$ such that $A_i = A_j$, $A_j | (i-j)$ and X_i, X_j do not exceed $\delta_3^{1/\ell}$. Also $\gcd(X_i, X_j) = 1$. Thus $(A_j X_j^\ell, A_j X_i^\ell) \in U_3(r)$ with $r = i - j$.

Furthermore, $d = A_j(X_i^\ell - X_j^\ell)/(i-j)$, which, by (2.9) and (2.10), implies that

$$M_{r,t}(A_jX_j^\ell, A_jX_i^\ell) = A_jX_j^\ell\left(1-\frac{t}{r}\right) + A_jX_i^\ell\ \frac{t}{r} = A_jX_j^\ell + td = n+(j+t)d.$$

If $0 \leqslant t \leqslant r$, we see that the left-hand side is a term of the product Δ and hence has Property P_0. Suppose that $r=1$. Then we take $0 \leqslant t \leqslant [\frac{k}{2}]$ if $0 \leqslant j \leqslant [\frac{k}{2}]-1$ and $-[\frac{k}{2}] \leqslant t \leqslant 0$ if $[\frac{k}{2}] \leqslant j \leqslant k-1$. Then $j+t \leqslant k-1$ in the former case and $j+t \geqslant 0$ in the latter case, implying that $M_{1,t}(A_jX_j^\ell, A_jX_i^\ell)$ is a term of the product Δ and therefore has Property P_0. Thus the triple $(A_jX_j^\ell, A_jX_i^\ell, r)$ has Property P_1. Hence $(A_jX_j^\ell, A_jX_i^\ell, r) \in U_4$. On the other hand, given k, ℓ as in (4.5), we check that for any pair $(hX^\ell, hY^\ell) \in U_3(r)$ with $1 < r < k$, Property P_0 does not hold for $M_{r,1}(hX^\ell, hY^\ell)$. When $r=1$, we check that $M_{1,1}(hX^\ell, hY^\ell)$ as well as $M_{1,-1}(hX^\ell, hY^\ell)$ do not have Property P_0. Thus, no triple (hX^ℓ, hY^ℓ, r) with $(hX^\ell, hY^\ell) \in U_3(r), 1 \leqslant r < k$ has Property P_1. Hence $U_4 = \emptyset$. This yields a contradiction.

We illustrate the above procedure with an example. Let $\ell = 11, k = 19$. Then we have $d \leqslant 10^{15}$ and $n+(k-1)d \leqslant 4\cdot 6 \times 10^{16}$ by (4.4). We form the set $U_2 = \{1, 23, 29, 31\}$. For each $1 \leqslant r < 19$, we construct $U_3(r)$. For instance, we have

$$U_3(17) = \{(1, 23^{11}), (1, 29^{11}), (1, 31^{11}), (23^{11}, 29^{11}), (23^{11}, 31^{11}), (29^{11}, 31^{11}), (17, 17\cdot 23^{11})\}.$$

We check that none of the triples (hX^ℓ, hY^ℓ, r) such that $(hX^\ell, hY^\ell) \in U_3(r)$ with $h|r$ for every $1 \leqslant r < 19$ has Property P_1. Thus $U_4 = \emptyset$, a contradiction. All other possibilities of ℓ and k in (4.5) are excluded similarly. □

5. Upper bound for $n+(k-1)d$ when ℓ is even

We use the method of Erdős [Erd39] to derive an upper bound for $n+(k-1)d$. We also refer thereafter to [SS03] for details.

Lemma 6. *Suppose that (1.1) is satisfied with $\ell \geqslant 4$ even. Let $h_0 = h_0(k)$ be a positive integer such that $h_0 = 1$ if $4 \leqslant k \leqslant 24$; $h_0 = 2$ if $25 \leqslant k \leqslant 74$; $h_0 = 4$ if $75 \leqslant k \leqslant 159$; $h_0 = 5$ if $k \geqslant 160$. Then $n < k^2d^2/(4h_0)$.*

Proof. Since ℓ is even we may write

$$n + id = b_iz_i^2 \quad \text{for } 0 \leqslant i < k \tag{5.1}$$

where b_i are square free with $P(b_i) \leqslant k$. Let R be the set of b_i. Suppose that $n \geqslant k^2d^2/(4h_0)$. First we show that $|R| \geqslant \min(k-2h_0+3, k)$. We say that an element b_j of R has multiplicity r_j if $b_j = b_i$ for r_j values of i. In particular, if b_j has multiplicity 1, then it means that b_j occurs only once and b_j is repeated only when it has multiplicity greater than 1. Suppose that $|R| \leqslant \min(k-2h_0+2, k-1)$. Then there are at least $\max(2, 2h_0-1)$ of the b_i counted with multiplicity that are repeated. Thus there exist b_i, b_j such that $b_i = b_j$ with $0 \leqslant i, j < k, i \neq j$. By (5.1) we assume without loss of generality that $z_i > z_j$ and

$$kd > (i-j)d \geqslant 2b_j(z_i - z_j)z_j \geqslant 2b_j^{1/2}(z_i-z_j)(b_jz_j^2)^{1/2} \geqslant 2b_j^{1/2}(z_i-z_j)n^{1/2}.$$

Hence $n < k^2d^2/(4b_j(z_i-z_j)^2)$. Thus $b_j(z_i-z_j)^2 < h_0$, implying that $h_0 > 1, b_j = z_i - z_j = 1$ if $h_0 = 2$, $b_j \in \{1,2,3\}$, $z_i - z_j = 1$ if $h_0 = 4$ and $b_j = 1$, $z_i - z_j = 1, 2$; $b_j \in \{2, 3\}$, $z_i - z_j = 1$ if $h_0 = 5$, by noting that b_j are square free. Therefore, there are at most $2h_0 - 2$ of the b_j counted with multiplicity that are repeated. This is a contradiction since $\max(2, 2h_0-1) = 2h_0 - 1$ by $h_0 > 1$. Thus we have $|R| \geqslant k - 2h_0 + 3$.

Since b_i are square free, we follow the argument of [SS03, (6.7), (6.9)] for $k-2h_0+3 \geqslant 63$ to get

$$(1.5)^{k-2h_0+3}(k-2h_0+3)! \leqslant \prod_{i=0}^{k-2h_0+4} b_i \leqslant 52k^8(k-1)!(1.0731)^k.$$

This implies that $k \leqslant 260$. Now we use the counting argument as in [SS03]. We explain with an example. Let $k = 260$. Then $h_0 = 5$ and $|R| \geqslant k-7$. We find that the number of distinct b_i composed of 2, 3, 5, 7, 11 is at least 37. On the other hand, since b_i are square free, this number is at most 32. This is a contradiction. Thus $k \neq 260$. We exclude all k with $160 \leqslant k < 260$ by the above argument. When $75 \leqslant k \leqslant 159$, we have $|R| \geqslant k-5$ and we see that the number of distinct b_i composed of 2, 3, 5, 7 exceed 16, which is a contradiction. Next, when $25 \leqslant k \leqslant 74$, we have $|R| \geqslant k-1$ and we find that the number of distinct b_i composed of 2, 3, 5 exceed eight giving a contradiction. Finally, when $4 \leqslant k \leqslant 24$, all b_j are distinct and by counting the b_i composed of $2, 3$, we get $k \leqslant 8$. Let $k = 8$. Then we see that b_2, b_3, b_4, b_5 are distinct and they are composed of 2 and 3. Therefore, these four b_i must take all the values of $\{1, 2, 3, 6\}$. Hence, the product of the corresponding terms in Δ must be a square. A result of Euler states that a product of four terms in an arithmetic progression is never a square. Dickson [Dic52, p. 635] gave a historical reference to Euler's result. We refer to [MS03] for a proof. Thus $k \neq 8$. Similarly, we see that $k \neq 4, 6$. Let $k = 7$. We have either 5 dividing b_0 and b_5 or 5 dividing b_1 and b_6. Suppose that 5 divides b_0 and b_5. Then 7 divides one of b_1, b_2, b_3, b_4 by the result of Euler stated above. Suppose that 7 divides b_2 or b_3. Since $(\frac{b_1}{5}) = (\frac{b_4}{5}) = (\frac{b_6}{5})$, we find that b_1, b_4, b_6 take values from $\{1, 6\}$ or $\{2, 3\}$, which is not possible since b_i are distinct. Thus 7 divides b_1 or b_4. If 7 divides b_1, then $(\frac{b_2}{7}) = (\frac{b_3}{7})$ and $(\frac{b_4}{7}) = (\frac{b_6}{7})$ implying that either $b_2, b_3 \in \{3, 6\}$ or $b_4, b_6 \in \{3, 6\}$, which is not possible. Likewise 7 dividing b_4 is excluded. The argument for the case 5 dividing b_1, b_6 is similar. Thus $k \neq 7$. Let $k = 5$. Then 5 divides one of b_1, b_2, b_3. Suppose that $5 \mid b_2$. Then $b_1, b_3 \in \{1, 6\}$, $b_0, b_4 \in \{2, 3\}$ or $b_1, b_3 \in \{2, 3\}$, $b_0, b_4 \in \{1, 6\}$. This is not possible. Thus $5 \nmid b_2$. Let $5 \mid b_1$. Then $(b_0, b_2, b_3, b_4) = (6, 1, 3, 2)$. Hence $n \equiv 6 \pmod 8$ and $n + 3d \equiv 3 \pmod 8$, which imply that $d \equiv 7 \pmod 8$. Therefore $n + 2d \equiv 4 \pmod 8$. When $5 \mid b_3$, we get $(b_0, b_1, b_2, b_4) = (2, 3, 1, 6)$ and $n + 2d \equiv 4 \pmod 8$. We consider the case $(b_0, b_2, b_3, b_4) = (6, 1, 3, 2)$. We have $3 \nmid z_2$. Suppose that $3 \mid z_0z_3$. Then we see from $n+2(n+3d) = 3(n+2d)$ that $2z_0^2+2z_3^2 = z_2^2$, which is impossible. Hence $3 \nmid z_0z_3$. Then we see from (2.8) that $(a_0, a_2, a_3, a_4) = (6, 4, 3, 2)$. Thus

$$nd + 6d^2 = (n+2d)(n+3d) - n(n+4d) = 12((x_2x_3)^\ell - (x_0x_4)^\ell),$$

which implies that $x_2x_3 > x_0x_4$. Hence

$$nd + 6d^2 > 12\ell(x_0x_4)^{\ell-1} = 12^{1/\ell}\ell(12x_0^\ell x_4^\ell)^{(\ell-1)/\ell} > 12^{1/\ell}\ell n^{2(\ell-1)/\ell}.$$

Thus

$$n^{(\ell-2)/\ell} < \frac{1}{12^{1/\ell}\ell}\left(d + \frac{6d^2}{n}\right) < \frac{1}{12^{1/\ell}\ell}(d+1)$$

since $n \geqslant 25d^2/4$. Thus $n < d^{\ell/(\ell-2)} \leqslant d^2$, a contradiction. The argument for the case $(b_0, b_2, b_3, b_4) = (2, 3, 1, 6)$ is similar. □

6. Upper bound for $n + (k-1)d$ when ℓ is odd

We assume in this section that ℓ is odd and we write $\ell = \ell_1^{e_1} \cdots \ell_r^{e_r}$ where ℓ_i are distinct primes and e_i are positive integers. We find an upper bound for $n + (k-1)d$ in Lemma 12 below, which is based on an extension of a result of Erdős and Selfridge on the distinctness of a_i and their products. See [ES75, Lemma 1] and [SS01, Lemmas 5 and 6]. We use the following well-known result on cyclotomic polynomials in this extension (see [Ste75]).

LEMMA 7. *For any integer $m > 2$ and relatively prime integers X, Y with $X > Y > 0$, let $\phi_m(X,Y)$ denote the mth cyclotomic polynomial. Then the prime divisors of $\phi_m(X,Y)$ are congruent to 1 $\pmod m$ except possibly $P(m)$ dividing it at most to the first power.*

As a consequence of Lemma 7, we get the following.

LEMMA 8. *Suppose that $Z_1 > Z_2 > 0$ are integers with $\gcd(Z_1, Z_2) = 1$ and*

$$\Phi_\ell(Z_1, Z_2) = \frac{Z_1^\ell - Z_2^\ell}{Z_1 - Z_2}.$$

Then every prime factor p of $\Phi_\ell(Z_1, Z_2)$ is either congruent to 1 $\pmod{\ell_i}$ for some i with $1 \leqslant i \leqslant r$ or $p = \ell_j$ for some j with $1 \leqslant j \leqslant r$. Furthermore, in the latter case, $\ell_j^{e_j} \parallel \Phi_\ell(Z_1, Z_2)$ provided ℓ_j is not congruent to 1 $\pmod{\ell_i}$ for any ℓ_i with $1 \leqslant i \leqslant r, i \neq j$.

Proof. First, we consider the case when ℓ is a prime power, i.e. $\ell = q^\alpha$ for some prime q and $\alpha > 0$. Then

$$\Phi_{q^\alpha}(Z_1, Z_2) = \frac{Z_1^{q^\alpha} - Z_2^{q^\alpha}}{Z_1 - Z_2} = \phi_q(Z_1, Z_2)\phi_q(Z_1^q, Z_2^q) \cdots \phi_q(Z_1^{q^{\alpha-1}}, Z_2^{q^{\alpha-1}}).$$

Hence, by Lemma 7, we see that every prime factor of $\Phi_{q^\alpha}(Z_1, Z_2)$ is congruent to 1 $\pmod q$ except perhaps q. When q divides any of the above cyclotomic polynomials, it divides each of them to the first power. Hence $q^\alpha \parallel \Phi_{q^\alpha}(Z_1, Z_2)$.

Now we consider any ℓ. We put $Z_{1,0} = Z_1$; $Z_{2,0} = Z_2$; for $i \geqslant 1$, $Z_{1,i} = Z_{1,i-1}^{\ell_i^{e_i}}$, $Z_{2,i} = Z_{2,i-1}^{\ell_i^{e_i}}$. Then we have

$$\Phi_\ell(Z_1, Z_2) = \Phi_{\ell_r^{e_r}}(Z_{1,r-1}, Z_{2,r-1})\Phi_{\ell_{r-1}^{e_{r-1}}}(Z_{1,r-2}, Z_{2,r-2}) \cdots \Phi_{\ell_1^{e_1}}(Z_{1,0}, Z_{2,0}).$$

Now the assertion follows by the case $\ell = q^\alpha$ from the previous paragraph. We note here that if ℓ_i divides $\Phi_{\ell_i^{e_i}}(Z_{1,i-1}, Z_{2,i-1})$ then $\ell_i^{e_i} \parallel \Phi_{\ell_i^{e_i}}(Z_{1,i-1}, Z_{2,i-1})$ and ℓ_i does not divide any other factor whenever ℓ_i is not congruent to 1 $\pmod{\ell_j}$ for any j with $1 \leqslant j \leqslant r, j \neq i$. Hence in that case, $\ell_i^{e_i} \parallel \Phi_\ell(Z_1, Z_2)$. □

Now we turn to an extension of a result of Erdős and Selfridge on the distinctness of a_i and their products. We write $d = D_1 D_2$ where D_1 is the maximal divisor of d such that every prime divisor of D_1 is congruent to 1 $\pmod{\ell_i}$ for some $\ell_i \mid \ell$. Thus every prime divisor of D_2 is incongruent to 1 $\pmod{\ell_i}$ for any $\ell_i \mid \ell$. We observe that D_1 and D_2 defined here agree with the definitions of D_1 and D_2 in [SS01] when ℓ is an odd prime. The following has been shown in [SS01].

LEMMA 9. *Let ℓ be an odd prime. Then (1.1) with $k \geqslant 4$ implies that*

$$D_1 > 1. \tag{6.1}$$

For $i \geqslant 1$, we set $\theta_i = 1/\ell_i^{\min(e_i, \operatorname{ord}_{\ell_i} D_2)}$ and

$$\theta = \theta_1 \cdots \theta_r. \tag{6.2}$$

We observe that $\theta = 1$ if $\gcd(\ell, d) = 1$. We show the following.

LEMMA 10. *Suppose that (1.1) holds. Let ℓ' be an integer with $1 \leqslant \ell' < \ell$. Furthermore, let*

$$D_1 \leqslant \frac{\ell\theta}{k\ell'} n^{(\ell-\ell')/\ell}. \tag{6.3}$$

Then for no distinct ℓ'-tuples $(i_1, \ldots, i_{\ell'})$ and $(j_1, \ldots, j_{\ell'})$ with $i_1 \leqslant \cdots \leqslant i_{\ell'}$ and $j_1 \leqslant \cdots \leqslant j_{\ell'}$, the ratio of the two products $a_{i_1} \cdots a_{i_{\ell'}}$ and $a_{j_1} \cdots a_{j_{\ell'}}$ is an ℓth power of a rational number.

Furthermore, for integers $m_1 \geqslant 1, m_2 \geqslant 0$ with $m_1 + m_2 \leqslant \pi(k)$, we have

$$\binom{H(d,k,m_1,m_2)+\ell'-1}{\ell'} \leqslant \ell^{m_1}\binom{\ell'+m_2}{\ell'} \tag{6.4}$$

where the left-hand side is zero if $H(d,k,m_1,m_2) < 1$.

Proof. We follow the argument of [SS01, Lemma 5]. Let $(i_1,\dots,i_{\ell'})$ and $(j_1,\dots,j_{\ell'})$ with $i_1 \leqslant \cdots \leqslant i_{\ell'}$ and $j_1 \leqslant \cdots \leqslant j_{\ell'}$ be distinct ℓ'-tuples such that

$$a_{i_1}\cdots a_{i_{\ell'}} = a_{j_1}\cdots a_{j_{\ell'}}\left(\frac{t_1}{t_2}\right)^{\ell}$$

where t_1 and t_2 are positive integers with $\gcd(t_1,t_2)=1$. As in the proof of [SS01, Lemma 5], we may assume that $(n+i_1d)\cdots(n+i_{\ell'}d) > (n+j_1d)\cdots(n+j_{\ell'}d)$ and

$$(n+i_1d)\cdots(n+i_{\ell'}d) - (n+j_1d)\cdots(n+j_{\ell'}d) = \frac{a_{j_1}\cdots a_{j_{\ell'}}}{t_2^{\ell}}(x^{\ell}-y^{\ell}) \tag{6.5}$$

where $x = t_1x_{i_1}\cdots x_{i_{\ell'}}, y = t_2x_{j_1}\cdots x_{j_{\ell'}}$ and $a_{j_1}\cdots a_{j_{\ell'}}/t_2^{\ell}$ is a positive integer. We rewrite (6.5) as

$$(n+i_1d)\cdots(n+i_{\ell'}d) - (n+j_1d)\cdots(n+j_{\ell'}d) = \frac{a_{j_1}\cdots a_{j_{\ell'}}}{t_2^{\ell}}\left(\frac{x^{\ell}-y^{\ell}}{x-y}\right)(x-y). \tag{6.6}$$

We observe that the left-hand side of (6.6) is divisible by d. Also by Lemma 8 and (6.2), we find that θD_2 divides $x-y$ since $\gcd(a_j,d)=1$ for $0 \leqslant j < k$. Thus $x \geqslant y + \theta D_2$. We estimate the left-hand side of (6.6) from above and the right-hand side of (6.6) from below as in [SS01, Lemma 6] to obtain

$$\left\{\binom{\ell}{1}\theta D_2 n^{\ell'(\ell-1)/\ell} - \binom{\ell'}{1}kdn^{\ell'-1}\right\} + \cdots + \left\{\binom{\ell}{\ell'}(\theta D_2)^{\ell'}n^{\ell'(\ell-\ell')/\ell} - (kd)^{\ell'}\right\} + \cdots + (\theta D_2)^{\ell} < 0. \tag{6.7}$$

By (6.3), we see that for each $1 \leqslant i \leqslant \ell'$ the term in the ith curly bracket above is positive. This is a contradiction to (6.7). Finally (6.4) follows as an immediate consequence from the argument [ES75, pp. 297–299]. See also [SS01, Lemma 6]. □

We apply Lemma 10 to get the following.

Lemma 11. *Suppose that (1.1) holds with $D_1 \leqslant (\ell\theta/2k)n^{(\ell-2)/\ell}$. Then $k < 11\,380$.*

Proof. Suppose that the hypothesis of Lemma 11 is satisfied. Then we observe that (6.3) is satisfied with $\ell' = 2$. Hence, by Lemma 10, we find that the products a_ia_j with $i \leqslant j$ are distinct. Then the estimates of [Sar97, Lemma 8] are valid. We use these estimates to conclude $k < 11\,380$ as in [Sar97, pp. 165–166]. □

Next we apply Lemmas 10 and 11 to bound n.

Lemma 12. *Suppose that (1.1) holds with ℓ odd. Then $n < (k\ell' D_1/\ell\theta)^{\ell/(\ell-\ell')}$ where ℓ' is given by Table 3 below. (For example, by Table 3, we understand that if $\ell = 7$, then $\ell' = 5$ for $4 \leqslant k \leqslant 8$ and $\ell' = 4$ for $k \geqslant 9$.)*

Proof. Suppose that (1.1) holds with $n \geqslant (k\ell' D_1/\ell\theta)^{\ell/(\ell-\ell')}$ where ℓ' is given in Table 3. Then (6.3) and the hypothesis of Lemma 11 are valid. Therefore, we derive from Lemmas 11 and 10 that $k < 11\,380$, a_i for $0 \leqslant i < k$ are distinct and (6.4) is valid. Now we proceed as in the proof of [SS01, Lemma 8]. We illustrate the proof with an example. Let $\ell = 5$. Then $\ell' = 4$ if $4 \leqslant k \leqslant 8$ and $\ell' = 3$ if $k \geqslant 9$ by Table 3. Let $k = 4$. Then, $H(d,4,2,0) \geqslant 4$ by Table 1. Hence (6.4) is not valid. Thus $k \neq 4$. Suppose that $k = 2958$. Then by Table 2, $m_1 = 4$, $m_2 = 12$ and $H(d,2958,4,12) \geqslant 271$.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

Table 3.

ℓ	$4 \leqslant k \leqslant 8$	$k \geqslant 9$	ℓ	$4 \leqslant k \leqslant 8$	$k \geqslant 9$
3	2	2	19	11	8
5	4	3	21	12	8
7	5	4	23	13	9
9	6	5	25	14	9
11	8	5	27	15	10
13	9	6	29	16	10
15	10	7	$\geqslant 31$	$(\ell+1)/2$	$(\ell+1)/2$
17	11	7	—	—	—

Table 4.

ℓ	k^*	ℓ	k^*
3	331	12	103
4, 6, 15, 16	23	17, 20	11
5, 7	317	18	13
8, 13, 14	47	19, 21–25, 27	7
9	53	26, 28, 29	5
10	19	30–37	4
11	113	—	—

Hence (6.4) is not valid. Thus $k \neq 2958$. We exclude all values of $k < 11\,380$ as above. The argument for excluding other values of $\ell \leqslant 29$ is similar. Let $\ell \geqslant 31$. Then $\ell' = (\ell+1)/2$ by Table 3. Let $Y = H_1(m_1)$ or $H_2(m_1, m_2)$. As above we need to show that (6.4) does not hold for $k < 11\,380$ and $\ell \geqslant 31$. We observe that if (6.4) does not hold for some odd $\ell = \ell_0$, then it does not hold for $\ell = \ell_0 + 2$ provided that

$$Y > \left(1 + \frac{2}{\ell_0}\right)^{m_1}(m_2+1) + \left(\frac{\ell_0+1}{2}\right)\left(\left(1+\frac{2}{\ell_0}\right)^{m_1} - 1\right). \tag{6.8}$$

We observe that the right-hand side of (6.8) is a decreasing function of ℓ_0. Hence, it is enough to check that (6.8) is valid and (6.4) is not valid at $\ell_0 = 31$. We carry out this by checking at $\ell_0 = 31$ for all $k < 11\,380$ and for m_1, m_2, Y as in Tables 1 and 2. □

7. Variables in (1.1) are bounded

Let $d \leqslant d_1$. We first bound ℓ and k. To do this, we compare the upper bound for $n + (k-1)d$ obtained in §§ 5 and 6 and the lower bound for $n + (k-1)d$ which can be obtained by using the iterative procedure in § 3. See Lemma 13. Let ℓ and k be given. Then we bound n by Lemmas 6 or 12 according to whether ℓ is even or odd, respectively. We observe that when n, d, k, ℓ are bounded, then b and y are also bounded by (1.1).

Lemma 13. *Assume (1.1) with Hypothesis A. Then $\ell \leqslant 37$ and $k \leqslant k^*$ with k^* given by Table 4.*

Proof. Assume (1.1) with Hypothesis A. Then all A_j are distinct by Corollary 1. Thus Lemma 3 is valid. Suppose that ℓ is even and $\ell \geqslant 38$. Then $d \leqslant k^{\ell-1}/2$. Hence in Lemma 3, we may take $\eta_i = \eta_i' = 0$ for every i. Furthermore, by (1.3) and Lemma 6, we get $\delta k^{\ell+1} = n + (k-1)d < k^2 d^2/(4h_0) + kd$. Thus

$$\delta < \frac{d^2}{4h_0 k^{\ell-1}} + \frac{d}{k^\ell}. \tag{7.1}$$

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

We observe that the right-hand side of (7.1) decreases as k or ℓ increases. Thus we evaluate the right-hand side at $k = 4$, $\ell = 38$ and $d = 10^{15}$ to get $\delta < 1.4 \times 10^7$. On the other hand, we see from Lemma 3 and a remark after the proof of (3.3) that $\delta > 4 \times 10^8$. Thus $\ell \leqslant 36$.

Let $\ell \leqslant 36$ be given. Suppose that $k > k^*$ where k^* is given in Table 4. We check that $d \leqslant k^{\ell-1}/2$ implying that $\eta_i = \eta_i' = 0$ for every i. Now we compute the lower bound of δ by Lemma 3 and the upper bound by (7.1) to see that they are inconsistent. Thus $k \leqslant k^*$.

Suppose that ℓ is odd and $\ell \geqslant 39$. Then $d \leqslant k^{\ell-1}/2$ and hence every $\eta_i = \eta_i' = 0$ in Lemma 3. Furthermore, by (1.3) and Lemma 12, we get

$$\delta k^{\ell+1} = n + (k-1)d < \left(\frac{k\ell' D_1}{\ell\theta}\right)^{\ell/(\ell-\ell')} + kd \tag{7.2}$$

where $\ell' = (\ell+1)/2$. By the definition of θ given by (6.2), we find that

$$\frac{D_1}{\theta} = D_1 \prod_{i=1}^{r} \ell_i^{\min(e_i, \mathrm{ord}_{\ell_i}(D_2))} \leqslant D_1 D_2 = d. \tag{7.3}$$

Thus, by (7.2) and (7.3), we get

$$\delta < \left(\frac{\ell' d}{\ell}\right)^{\ell/(\ell-\ell')} k^{-\ell+\ell'/(\ell-\ell')} + \frac{d}{k^\ell}. \tag{7.4}$$

Replacing ℓ' by $(\ell+1)/2$ in (7.4), we get

$$\delta < \left(\frac{(\ell+1)d}{2\ell}\right)^{2\ell/(\ell-1)} k^{(-\ell^2+2\ell+1)/(\ell-1)} + \frac{d}{k^\ell}. \tag{7.5}$$

We observe that the right-hand side of (7.5) decreases as k or ℓ increases. Hence, we evaluate the right-hand side of (7.5) at $\ell = 39$, $k = 4$ and $d = 10^{15}$ to find that $\delta < 2.3 \times 10^7$. On the other hand, we get $\delta \geqslant 7 \times 10^8$ for $k \geqslant 4$ by Lemma 3. This is a contradiction. Thus $\ell \leqslant 37$. Let $\ell \leqslant 37$ be given. Suppose that $k > k^*$ where k^* is given in Table 4. We check that $d \leqslant k^{\ell-1}/2$ implying that $\eta_i = \eta_i' = 0$ for every i. Now we compute the lower bound for δ by Lemma 3. Next we turn to an upper bound for δ. For this, we use (7.4) with ℓ' given by Table 3 when $5 \leqslant \ell \leqslant 29$ and we use (7.2) if $\ell = 3$. We observe that (7.5) holds when $31 \leqslant \ell \leqslant 37$ since $\ell' = (\ell+1)/2$. Finally, we check that the lower bound and the upper bound for δ obtained above are inconsistent. □

8. Algorithm for solving (1.1) when d is large

In this section, we present an algorithm for finding the solutions of (1.1) whenever $k, \ell, d' > 0$, $\delta_1 > 0$, $\delta_2 > 0$ are given such that $1 < d \leqslant d'$ and $\delta_1 < \delta < \delta_2$. We choose $m_1, \alpha_1, \dots, \alpha_{m_1}$ suitably and compute G_0 given by (2.18). We put

$$\kappa = \begin{cases} \left[\dfrac{k}{G_0 - 2}\right] & \text{if } G_0 \geqslant 3; \\ k & \text{otherwise} \end{cases} \quad \text{and} \quad a = p_1^{\alpha_1 - 1} \cdots p_{m_1}^{\alpha_{m_1} - 1}. \tag{8.1}$$

Below, we give the various steps of the algorithm.

Algorithm 1.

Step 1. We form the set W_1 of divisors of a.

Step 2. We form the set W_2 of pairs (AZ_1^ℓ, BZ_2^ℓ) such that $A, B \in W_1$ with $A < B$, $\gcd(A, B) = 1$, Z_2/Z_1 is a convergent in the continued fraction expansion of $(A/B)^{1/\ell}$, Z_1, Z_2 do not exceed $\delta_2^{1/\ell} k^{1+1/\ell}$, least prime factor of $Z_1 Z_2 > k$ if $G_0 \geqslant 3$ and $P(Z_1 Z_2) > k$ if $G_0 < 3$ and $((\delta_1 k^{\ell+1} - kd')/a)^{1/\ell} < Z_1$.

Step 3. Let

$$\delta_1 k^\ell - d' \leqslant (2\kappa d')^{\ell/(\ell-2)}. \tag{8.2}$$

Then we carry out (A)–(C) as given below.

(A) We form the set W_3 of all positive integers that are ℓth powers having all prime factors greater than k and not exceeding δ_4, where $\delta_4 \leqslant \min((3\kappa d')^{\ell/(\ell-2)}, \delta_2 k^{\ell+1})$. We observe that W_3 contains 1. We take $W_4 = W_3 - \{1\}$ if $G_0 \geqslant 3$ and $W_4 = W_3$ otherwise.

(B) Let W_5 be the set of integers of the form AZ^ℓ with $A \in W_1, Z^\ell \in W_4$ such that $\delta_1 k^\ell - d' \leqslant AZ^\ell \leqslant \delta_4$. Let the elements of W_5 be arranged in increasing order. Let $W_5(i)$ denote the ith element of W_5.

(C) Let W_6 be the set of pairs $(W_5(j), W_5(i))$ with $\gcd(W_5(j), W_5(i)) = 1$, $P(W_5(j)$ $W_5(i)) > k$ if $G_0 < 3$ and $W_5(i) - W_5(j) < \kappa d'$ for $1 \leqslant j < i \leqslant |W_5|$.

Step 4. We form $W_7 = W_2$ if (8.2) does not hold and $W_7 = W_2 \cup W_6$ otherwise.

Step 5. Let W_8 be the set of pairs $(N_1, N_2) \in W_7$ for which the triple $(N_1, N_2, 1)$ has Property P_2. Let W_9 be the set of pairs $(N_1, N_2) \in W_8$ for which the triple (N_1, N_2, r) has Property P_1 for some integer $r \geqslant 1$ dividing $N_2 - N_1$.

Now we show that under suitable conditions $W_9 \neq \emptyset$ whenever (1.1) holds.

LEMMA 14. *Suppose that (1.1) with Hypothesis A holds. Let $k \geqslant 4$, $G_0 \geqslant 2$ and $\delta_1 k^\ell \geqslant a$. Then $W_9 \neq \emptyset$ where W_9 is constructed as in the algorithm with $d' = d_1$.*

Proof. Assume (1.1) with Hypothesis A. By Corollary 1, all the A_i are distinct. Therefore, there are at least G_0 of the A_i in W_1, which are composed of $p_1, \ldots, p_{m_1}$ to the orders not exceeding $\alpha_1 - 1, \ldots, \alpha_{m_1} - 1$, respectively. Suppose that $G_0 \geqslant 3$. Then we divide the interval $[0, k)$ into $G_0 - 2$ sub intervals

$$\left[0, \frac{k}{G_0 - 2}\right), \ldots, \left[\frac{(G_0 - 3)k}{G_0 - 2}, k\right) \tag{8.3}$$

of length $k/(G_0 - 2)$. We find that there exists a sub interval from (8.3) containing two integers $0 < i_0 < j_0 < k$ such that A_{i_0}, A_{j_0} are in W_1. Since $G_0 \geqslant 2$ there always exist two terms of Δ, say, $n + id = A_i X_i^\ell$ and $n + jd = A_j X_j^\ell$ with $j > i$ and A_i, A_j in W_1. By (8.1), we find

$$(j - i)d = A_j X_j^\ell - A_i X_i^\ell \quad \text{with } 0 < j - i < \kappa \tag{8.4}$$

where $i > 0$ whenever $G_0 \geqslant 3$. Suppose that $X_j = 1$. Then since $j > 0$, we have $a \geqslant A_j = A_j X_j^\ell = n + jd > d$. Hence, $a \geqslant n + jd > n > \delta_1 k^{\ell+1} - (k-1)d > \delta_1 k^{\ell+1} - (k-1)a$ contradicting our assumption. Thus $X_j \neq 1$. Similarly, we see that $X_i \neq 1$ whenever $i \neq 0$. Thus we always have $P(X_i X_j) > k$ and if $G_0 \geqslant 3$, then the least prime factor of $X_i X_j > k$. We note that A_i, A_j are coprime to d. Hence by (8.4), we get

$$\alpha = \gcd(A_i, A_j) < k. \tag{8.5}$$

Furthermore, we put $A'_i = \alpha^{-1} A_i$, $A'_j = \alpha^{-1} A_j$. By dividing both sides of (8.4) by $\gcd(A_i, A_j)$, we get

$$A'_\mu X_\mu^\ell - A'_\nu X_\nu^\ell = \pm r d \tag{8.6}$$

where $0 < r < \kappa/\alpha$, $(\mu, \nu) = (i, j)$ or (j, i), $A'_\mu > A'_\nu$ are in W_1 and $\gcd(A'_\mu, A'_\nu) = 1$. Furthermore, by (8.5), we see that

$$\delta_1 k^\ell - d_1 < A'_\mu X_\mu^\ell, A'_\nu X_\nu^\ell < \delta_2 k^{\ell+1}. \tag{8.7}$$

Therefore X_μ, X_ν do not exceed $\delta_2^{1/\ell} k^{1+1/\ell}$ and they are bounded from below by $((\delta_1 k^{\ell+1} - kd_1)/a)^{1/\ell}$. Suppose that (8.2) does not hold. Then we find by (8.7) that

$$A'_\nu X_\nu^{\ell-2} \geqslant (A'_\nu X_\nu^\ell)^{(\ell-2)/\ell} > (\delta_1 k^\ell - d_1)^{(\ell-2)/\ell} > 2\kappa d_1. \tag{8.8}$$

From (8.6) we get

$$\left| \frac{A'_\nu}{A'_\mu} - \frac{X_\mu^\ell}{X_\nu^\ell} \right| < \frac{\kappa d_1}{A'_\mu X_\nu^\ell}$$

which, by (8.8), implies that

$$\left| \left(\frac{A'_\nu}{A'_\mu}\right)^{1/\ell} - \frac{X_\mu}{X_\nu} \right| < \frac{\kappa d_1}{A'_\mu X_\nu^\ell} \left(\frac{A'_\mu}{A'_\nu}\right)^{1-1/\ell} < \frac{\kappa d_1}{A'_\nu X_\nu^\ell} < \frac{1}{2X_\nu^2}.$$

Thus X_μ/X_ν is a convergent in the continued fraction expansion of $(A'_\nu/A'_\mu)^{1/\ell}$, see [NZ80, p. 161]. Hence $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell) \in W_2 = W_7$. We observe that $\alpha A'_\nu X_\nu^\ell, \alpha A'_\mu X_\mu^\ell$ are two terms of Δ and hence the triple $(\alpha A'_\nu X_\nu^\ell, \alpha A'_\mu X_\mu^\ell, \alpha r)$ has Property P_1. Since $\alpha < k$, we conclude that the triple $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell, r)$ has Property P_1. Furthermore, we observe that $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell, 1)$ also has Property P_2. Thus the pair $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell) \in W_9$, which proves the assertion.

Thus we may suppose that (8.2) holds. Furthermore, if $A'_\nu X_\nu^{\ell-2} > 2\kappa d_1$, then we argue as in the previous paragraph to see that $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell) \in W_9$ yielding the assertion. Thus, we may suppose that $A'_\nu X_\nu^{\ell-2} \leqslant 2\kappa d_1$. Hence

$$A'_\nu X_\nu^\ell \leqslant (A'_\nu X_\nu^{\ell-2})^{\ell/(\ell-2)} \leqslant (2\kappa d_1)^{\ell/(\ell-2)}, \tag{8.9}$$

which, together with (8.7), implies that $A'_\nu X_\nu^\ell \in W_5$. Let $A'_\nu X_\nu^\ell = W_5(i)$ for some $i \geqslant 1$. We see from (8.9) and (8.6) that $A'_\mu X_\mu^\ell \leqslant A'_\nu X_\nu^\ell + \kappa d_1 \leqslant (3\kappa d_1)^{\ell/(\ell-2)}$ and hence $A'_\mu X_\mu^\ell \in W_5$. Thus by (8.6), the pair $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell) \in W_6$. Arguing as earlier, we see that $(A'_\nu X_\nu^\ell, A'_\mu X_\mu^\ell) \in W_9$ which proves the assertion. □

9. Proof of Theorem 1 when $\ell > 3$

We assume (1.1) with Hypothesis A and $\ell > 3$. Then $k \geqslant 4$. By Lemma 13, we see that $\ell \leqslant 37$ and $k \leqslant k^*$ with k^* given by Table 4. We apply Algorithm 1 with $d' = d_1$ to exclude all of these values of ℓ and k as follows. For all values of ℓ, we choose $m_1, \alpha_1, \ldots, \alpha_{m_1}$, as below. We give the choices for $k \leqslant k^*$, k prime or $k = 4$.

$k = 4$: $m_1 = 2, \alpha_1 = \alpha_2 = 2$;

$5 \leqslant k \leqslant 10$: $m_1 = 2$, $\alpha_1 = 3$, $\alpha_2 = 2$;

$11 \leqslant k \leqslant 28$: $m_1 = 3$, $\alpha_1 = 4$, $\alpha_2 = \alpha_3 = 2$;

$29 \leqslant k \leqslant 36$: $m_1 = 3$, $\alpha_1 = 4$, $\alpha_2 = 3$, $\alpha_3 = 2$;

$37 \leqslant k \leqslant 66$: $m_1 = 3$, $\alpha_1 = 5$, $\alpha_2 = 3$, $\alpha_3 = 2$;

$67 \leqslant k \leqslant 100$: $m_1 = 4$, $\alpha_1 = 4$, $\alpha_2 = 3$, $\alpha_3 = \alpha_4 = 2$;

$101 \leqslant k \leqslant 198$: $m_1 = 5$, $\alpha_1 = 4$, $\alpha_2 = 3$, $\alpha_3 = \alpha_4 = \alpha_5 = 2$;

$199 \leqslant k \leqslant 270$: $m_1 = 5$, $\alpha_1 = 5$, $\alpha_2 = 3$, $\alpha_3 = \alpha_4 = \alpha_5 = 2$;

$271 \leqslant k \leqslant 331$: $m_1 = 5$, $\alpha_1 = 5$, $\alpha_2 = \alpha_3 = 3$, $\alpha_4 = \alpha_5 = 2$.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

By these choices of $m_1, \alpha_1, \ldots, \alpha_{m_1}$, we find that $G_0 \geqslant 4$ except for $k = 4, 5, 7, 19, 23$ in which cases $G_0 = 2, 2, 2, 3, 3$, respectively. By (2.7) and $\ell \geqslant 4$, we see that $\delta > \delta_1$ where $\delta_1 k^\ell \geqslant p^4_{\pi(k)+\chi_0}/k \geqslant a$ with a given by (8.1). Thus the conditions of Lemma 14 are satisfied. We now explain the rest of the algorithm by means of an example.

We take $\ell = 5$. Then $d_1 = 5 \cdot 10^4$ and $k^* = 317$. For every $k \leqslant k^*$, we compute G_0 and by Lemma 3, we find δ_1. We observe that (8.2) is valid only for $k \leqslant 61$. Thus

$$W_7 = \begin{cases} W_2 \cup W_6 & \text{for } 4 \leqslant k \leqslant 61, \\ W_2 & \text{for } 67 \leqslant k \leqslant 317. \end{cases} \tag{9.1}$$

We fix $k = 11$. Then $m_1 = 3$, $\alpha_1 = 4$, $\alpha_2 = \alpha_3 = 2$ and $G_0 = 4$. Thus $\kappa = 5$, $a = 2^3 \cdot 3 \cdot 5$. We apply Lemma 3 to get $\delta > 7 = \delta_1$. By Lemma 12, we find that

$$\frac{n + (k-1)d}{k^6} \leqslant ((33 \cdot 10^4)^{5/2} + 5 \cdot 10^5)/11^6 < 35\,312\,523 = \delta_2.$$

By (9.1), we need to form the sets W_2 as well as W_6. As in Step 1, we first form the set W_1 of divisors of $2^3 \cdot 3 \cdot 5$. Then we form the set W_2. For this, we fix (A, B) with

$$A, B \in W_1, A < B, \ \gcd(A, B) = 1. \tag{9.2}$$

Next we find all integers Z_1, Z_2 such that $Z_1, Z_2 \leqslant \delta_2^{1/5} 11^{6/5} \leqslant 575$, $Z_1 > ((7 \cdot 11^6 - 5 \cdot 10^5)/2^3 \cdot 3 \cdot 5)^{1/5} > 9$, the least prime factor of $Z_1 Z_2 > 11$ and Z_2/Z_1 is a convergent in the continued fraction expansion of $(A/B)^{1/5}$. Then we form the set $W_2(A, B)$ of all pairs (AZ_1^5, BZ_2^5). Finally we put $W_2 = \bigcup W_2(A, B)$ where the union is taken over all the pairs (A, B) satisfying (9.2). We get

$$W_2 = \{(47^5, 2^3 \cdot 31^5), \ (3 \cdot 19^5, 2^2 \cdot 5 \cdot 13^5)\}. \tag{9.3}$$

We proceed to carry out Step 3 (A)–(C). We have $\delta_4 = 6.2 \times 10^9$. Thus W_3 is the set of integers of the form Z^5 with the least prime factor of Z exceeding 11 and $Z \leqslant 90$. Hence, W_4 is the set of fifth powers of all primes greater than 11 and less than or equal to 89. Then W_5 is the set of integers of the form AZ^5 with $A \in W_1$, $Z^5 \in W_4$ such that $1\,077\,357 \leqslant \delta_1 k^\ell - d_1 \leqslant AZ^\ell \leqslant 6.2 \times 10^9$. Now we find all pairs $(W_5(j), W_5(i))$ with $\gcd(W_5(j), W_5(i)) = 1$ and $W_5(i) - W_5(j) \leqslant \kappa d_1 = 25 \cdot 10^4$ for $1 \leqslant j < i \leqslant |W_5|$. We get

$$W_6 = \{(2^2 \cdot 13^5, 17^5), (19^5, 2 \cdot 3 \cdot 13^5), (2^2 \cdot 17^5, 3 \cdot 5 \cdot 13^5), (3 \cdot 19^5, 2^2 \cdot 5 \cdot 13^5), (31^5, 2^2 \cdot 5 \cdot 17^5)\}. \tag{9.4}$$

Then W_7 is the union of the sets in (9.3) and (9.4). Among the pairs (N_1, N_2) in W_7, we find that Property P_2 holds for $(N_1, N_2, 1)$ only when (N_1, N_2) is in the set

$$W_8 = \{(19^5, 2 \cdot 3 \cdot 13^5), (2^2 \cdot 17^5, 3 \cdot 5 \cdot 13^5), (31^5, 2^2 \cdot 5 \cdot 17^5)\}.$$

For each pair (N_1, N_2) in W_8, we check that the triple (N_1, N_2, r) does not have Property P_1 for any integer $r \geqslant 1$ dividing $N_2 - N_1$. Thus $W_9 = \emptyset$, which is not possible by Lemma 14. Thus $k \neq 11$. All other values of k with $4 \leqslant k \leqslant 317$ are excluded similarly. Finally we exclude all other values of ℓ as above. □

10. Algorithm for solving (1.1) when d is small

We give an algorithm for finding solutions of (1.1) when d is small and this is more efficient than Algorithm 1. This algorithm is a modified extension of the algorithm given in [SS03]. Let k, ℓ, $d' > 0, \delta_1 > 0, \delta_2 > 0$ be given such that $1 < d \leqslant d'$ and $\delta_1 < \delta < \delta_2$. Let d be fixed. We now give the various steps of the algorithm.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

Algorithm 2.

Step 1′. We have $n + (k-1)d > \delta_1 k^{\ell+1}$. We use (3.1) if $d \geqslant \delta_1 k^{\ell}/2$ and, otherwise, we use (3.2) to estimate $|I| \geqslant \alpha'$, say. Let $\chi_1 = \max(\alpha', 2)$ and $p_{\pi(k)+\chi_1} = Q_0$. For any integer $i > 0$, we put

$$s_1(i) = \left[\frac{\delta_1 k^{\ell+1} - kd}{i^{\ell}}\right] + 1; \quad s_2(i) = \left[\frac{\delta_2 k^{\ell+1}}{i^{\ell}}\right];$$
$$s_3(i) = \left[\frac{Q_0^{\ell} k^{\ell}}{i^{\ell}}\right] + 1; \quad s_4(i) = \min(s_2(i), s_3(i)).$$

Now we find all primes Q such that

$$Q_0 \leqslant Q \leqslant \min(Q_0 k, \delta_2^{1/\ell} k^{1+1/\ell}). \tag{10.1}$$

For each Q in (10.1) we form the set

$$D'_Q = \{t\, Q^l \mid \gcd(t\, Q^l, d) = 1, P(t) \leqslant k, s_1(Q) \leqslant t \leqslant s_4(Q)\}.$$

We put $E' = \bigcup D'_Q$ where the union is taken over all Q satisfying (10.1). Furthermore, if $Q_0 < (\delta_2 k)^{1/\ell}$, then we find all primes Q such that

$$Q_0 \leqslant Q \leqslant \delta_2^{1/\ell} k^{1+1/\ell}. \tag{10.2}$$

For each Q in (10.2) we form the set

$$D''_Q = \{t\, Q^l \mid \gcd(t\, Q^l, d) = 1, s_3(Q) \leqslant t \leqslant s_2(Q) \text{ and } t\, Q^l \text{ has Property } P_0\}.$$

We put $E'' = \bigcup D''_Q$ where the union is taken over all Q satisfying (10.2). Finally we put

$$E_d = E' \cup E'' \quad \text{if } Q_0 < (\delta_2 k)^{1/\ell}; \quad E = E' \quad \text{otherwise.}$$

Step 2′. Let $E_{d,0} = E_d$. We take $E'_{d,1}$ to be the set of $N \in E_{d,0}$ for which $N + d$ as well as $N - d$ do not have Property P_0. We put $E_{d,1} = E_{d,0} - E'_{d,1}$. Next, we construct $E'_{d,2}$ to be the set of $N \in E_{d,1}$ for which $N + 2d$ does not have Property P_0 and at least one of $N - d$, $N - 2d$ does not have Property P_0. We put $E_{d,2} = E_{d,1} - E'_{d,2}$. We proceed inductively to construct the sets $E'_{d,3}, E_{d,3}, \dots$. We observe that

$$E_{d,0} \supseteq E_{d,1} \supseteq E_{d,2} \supseteq \cdots . \tag{10.3}$$

Thus, $N \in E_{d,i}$ implies that $N \notin E'_{d,i}$ which means that either $N + id$ has Property P_0 or every one of $N - d, N - 2d, \dots, N - id$ has Property P_0.

Step 3′. We construct the sequence (10.3) for every $d \leqslant d'$.

Lemma 15. *Assume (1.1) with Hypothesis A. Let $k \geqslant 4$ and $\delta_1 < \delta < \delta_2$. Suppose that $d \leqslant d_1$ is fixed. Then $E_{d,i} \neq \emptyset$ for $1 \leqslant i \leqslant [\frac{k}{2}]$.*

Proof. Assume (1.1) with Hypothesis A and let $\delta_1 < \delta < \delta_2$. Then we see that there is a term in Δ, say $n + hd$, $0 \leqslant h < k$ which is divisible by a prime $Q_1 \geqslant p_{\pi(k)+\chi_1} = Q_0$ to an ℓth power. Thus $n + hd = t_1 Q_1^{\ell}$ where t_1 is a positive integer. Furthermore, $\gcd(t_1 Q_1^l, d) = 1$ since $\gcd(n, d) = 1$. Suppose that $Q_0 \geqslant (\delta_2 k)^{1/\ell}$. Then $t_1 \delta_2 k \leqslant t_1 Q_0^{\ell} \leqslant t_1 Q_1^{\ell} < \delta_2 k^{\ell+1}$ implying $t_1 < k^{\ell}$. Since $t_1 Q_1^{\ell}$ is a term of Δ, it has Property P_0. Hence $P(t_1) \leqslant k$. Furthermore, since $\delta_1 < \delta < \delta_2$ and $Q_0^{\ell} k^{\ell} \geqslant \delta_2 k^{\ell+1}$, we have $s_1(Q_1) \leqslant t_1 \leqslant [\delta_2 k^{\ell+1}/Q_1^{\ell}] = s_4(Q_1)$. Also Q_1 satisfies (10.1). Thus $t_1 Q_1^{\ell} \in E'$. Suppose that $Q_0 < (\delta_2 k)^{1/\ell}$. If $t_1 Q_1^{\ell}$ satisfies $Q_0^{\ell} k^{\ell} < t_1 Q_1^{\ell} < \delta_2 k^{\ell+1}$, then we see that $t_1 Q_1^{\ell} \in E''$. If $t_1 Q_1^{\ell} \leqslant Q_0^{\ell} k^{\ell}$, then $t_1 Q_1^{\ell} \in E'$. Hence $n + hd \in E_{d,0}$. By (1.1), we see that $n + (h + j)d$ has Property P_0 for $0 \leqslant j < k - h$. Also $n + (h - j)d$ has Property P_0 for $0 \leqslant j \leqslant h$. Let $h \leqslant [k/2]$. Then $n + hd \in E_{d,i}$ for every $0 \leqslant i \leqslant [k/2]$ since $k = 4$ or k is prime. Suppose that $[k/2] < h < k$. Then we consider $n+(h-[k/2])d = n+h'd$ with $0 < h' \leqslant [k/2]$. We see that $n+h'd$ is a term of Δ and arguing as earlier we get $n+h'd \in E_{d,i}$ for every $0 \leqslant i \leqslant [k/2]$. This proves the assertion. $\square$

11. Proof of Theorem 1 when $\ell = 3$

We assume (1.1) with Hypothesis A and $\ell = 3$. Let $k \geqslant 4$. Then by Lemma 9, we have

$$d \in \{7, 13, 14, 19, 21, 26, 28\}. \tag{11.1}$$

Furthermore, by (7.2) and Lemma 3, we see that k is bounded above by $47, 131, 47, 263, 331, 131, 47$ according as $d = 7, 13, 14, 19, 21, 26, 28$, respectively. We apply Algorithm 2 to exclude all of these values of k and d. We explain by means of examples. Let $d = 19$. First we take $k = 109$. By Lemma 3, we see that $\delta > 4.8804 = \delta_1$. By (7.2), we get $\delta < 18.65 = \delta_2$. We compute $\chi_1 = \alpha' = 56$. Thus $Q_0 = 439$. We see that $Q_0 > (\delta_2 k)^{1/\ell}$. Thus we need to compute $E_d = E'$. First we find all the primes Q between 439 and 1380. Then we form D'_Q. For instance, when $Q = 439$, we get $s_1(Q) = 9$, $s_4(Q) = 31$ and $D'_{439} = \{t\ 439^3 | 9 \leqslant t \leqslant 31, t \neq 19\}$. We now construct E_d and follow Step 2′. We find that $E_{d,1} = \{3^2 \cdot 479^3, 2 \cdot 7 \cdot 449^3, 2 \cdot 3 \cdot 751^3\}$ and $E_{d,2} = \emptyset$. This contradicts Lemma 15. Thus $k \neq 109$. Next we take $k = 4$. Then $\delta > 1.339 = \delta_1$. By (7.2), we get $\delta < 509 = \delta_2$. Furthermore, $\chi_1 = \alpha' = 2$. Thus $Q_0 = 7$. We see that $Q_0 < (4 \times 509)^{1/3}$. Thus we need to compute $E_d = E' \cup E''$. For the primes between 7 and 23, we compute D'_Q as well as D''_Q. For primes between 29 and 47, we compute D''_Q. For instance, suppose $Q = 29$, then we find that $s_3(Q) = 1$, $s_2(Q) = 5$ and $D''_Q = \{t\ 29^3 | 1 \leqslant t \leqslant 5, t \neq 5\}$. We follow Step 2′ to get $E_{d,1} = \emptyset$. Thus $k \neq 4$. All other values of k are excluded similarly. We exclude all the values of d in (11.1) as above.

Let $k = 3$. By the result of Győry [Győ99], we have $3 \nmid d$. Now we omit the one term in Δ divisible by 3. Then we see from (1.1) that

$$N(N+id) = b'_1 y_1^3, \quad i = 1, 2, \quad b'_1 = 1, 2, 4, \tag{11.2}$$

where $N = n$ or $n+d$ if $i = 1$, $N = n$ if $i = 2$ and y_1 is some positive integer. Suppose that d is even. Then N and $N+id$ are both odd and by (11.2) we have $N = u^3, N+id = v^3$ for some positive integers u and v. Thus $60 \geqslant id = v^3 - u^3$ implying that $(u,v) = (1,3)$. Thus $n = 1, d = 26$, which is not possible by (1.1). Hence, we may assume that d is odd. Thus

$$d \in \{5, 7, 11, 13, 17, 19, 23, 25, 29\}. \tag{11.3}$$

We put $X_1 = N + id/2$. Then (11.2) becomes $X_1^2 - i^2d^2/4 = b'_1 y_1^3$. We see that this equation can be rewritten as $X^2 = Y^3 + (b'_2 d)^2$ with $b'_2 \in \{1, 2, 4\}$. Now we use SIMATH to find all the integral solutions of this elliptic equation when d is given by (11.3). We check that none of the integral solutions yield any solution to (1.1). $\square$

References

Dic52 L. E. Dickson, *History of the theory of numbers*, vol. II (Chelsea, New York, 1952).

DG95 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.

Erd39 P. Erdős, *Note on the product of consecutive integers (II)*, J. London Math. Soc. (2) **14** (1939), 245–249.

ES75 P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.

FH01 P. Filakovszky and L. Hajdu, *The resolution of the Diophantine equation $x(d+d)\cdots(x+(k-1)d) = by^2$ for fixed d*, Acta Arith. **98** (2001), 151–154.

Győ98 K. Győry, *On the Diophantine equation $n(n+1)\cdots(n+k-1) = bx^\ell$*, Acta Arith. **83** (1998), 87–92.

https://doi.org/10.1112/S0010437X04001125 Published online by Cambridge University Press

Győ99 K. Győry, *Power values of products of consecutive integers and binomial coefficients*, in *Number theory and its applications* (Kyoto, 1997), Dev. Math., vol. 2 (Kluwer, Dordrecht, 1999), 145–156.

Mar85 R. Marszalek, *On the product of consecutive elements of an arithmetic progression*, Monatsh. Math. **100** (1985), 215–222.

MS03 A. Mukhopadhyay and T. N. Shorey, *Almost squares in arithmetic progression II*, Acta Arith. **110** (2003), 1–14.

NZ80 I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, fourth edition (Wiley, New York, 1980).

RS62 B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

Sar97 N. Saradha, *On perfect powers in products with terms from arithmetic progressions*, Acta Arith. **82** (1997), 147–172.

Sar98 N. Saradha, *Squares in products with terms in an arithmetic progression*, Acta Arith. **86** (1998), 27–43.

Sho00 T. N. Shorey, *Exponential Diophantine equations involving products of consecutive integers and related equations*, in *Number Theory*, eds R. P. Bambah, V. C. Dumir and R. J. Hans-Gill, Trends Math. (Birkhäuser, Basel, 2000), 463–495.

Sho02a T. N. Shorey, *Powers in arithmetic progression*, in *A panorama in number theory or the view from Baker's garden*, ed. G. Wüstholz (Cambridge University Press, Cambridge, 2002), 325–336.

Sho02b T. N. Shorey, *Powers in arithmetic progression II*, in *New aspects of analytic number theory* (Kyoto, 2001), Sūrikaisekikenkyūshu Kōkyūroku, vol. 1274 (Kyoto University, Kyoto, 2002).

SS01 N. Saradha and T. N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. **99** (2001), 363–388.

SS03 N. Saradha and T. N. Shorey, *Almost squares in arithmetic progression*, Compositio Math. **138** (2003), 73–111.

SST02 N. Saradha, T. N. Shorey and R. Tijdeman, *Some extensions and refinements of a theorem of Sylvester*, Acta Arith. **102** (2002), 167–181.

ST90 T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression. A tribute to Paul Erdős*, eds A. Baker, B. Bollobás and A. Hajnal (Cambridge University Press, Cambridge, 1990), 385–389.

Ste75 C. L. Stewart, *The greatest prime factor of* $a^n - b^n$, Acta. Arith. **26** (1975), 427–433.

Tij89 R. Tijdeman, *Diophantine equations and Diophantine approximations*, in *Number Theory and Applications* (Banff, 1988) (Kluwer, Dordrecht, 1989), 215–243.

N. Saradha saradha@math.tifr.res.in

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India

T. N. Shorey shorey@math.tifr.res.in

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India