COMPOSITIO MATHEMATICA

T. N. SHOREY
R. TIJDEMAN

Perfect powers in products of terms in an arithmetical progression

Compositio Mathematica, tome 75, nº 3 (1990), p. 307-344
<http://www.numdam.org/item?id=CM_1990__75_3_307_0>

Compositio Mathematica **75**: 307–344, 1990.

Perfect powers in products of terms in an arithmetical progression

T. N. SHOREY[1] and R. TIJDEMAN[2]

[1] *School of Mathematics, Taba Institute of Fundamental Research, Homi Bhabha Road, Bombay 400005, India;* [2] *Mathematical Institute, R.U. Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands*

Received 27 December 1988; accepted in revised form 14 February 1990

Dedicated to the memory of Professor Th. Schneider

1. Introduction

For an integer $x > 1$, we denote by $P(x)$ the greatest prime factor of x and we write $\omega(x)$ for the number of distinct prime divisors of x. Further, we put $P(1) = 1$ and $\omega(1) = 0$. We consider the equation

$$m(m + d) \cdots (m + (k - 1)d) = by^l \tag{1.1}$$

in positive integers, b, d, k, l, m, y subject to $P(b) \leqslant k$, $\gcd(m, d) = 1$, $k > 2$, $l \geqslant 2$. There is no loss of generality in assuming that l is a prime number. We shall follow this notation without reference. Erdös conjectured that equation (1.1) with $b = 1$ implies that k is bounded by an absolute constant and later he conjectured that even $k \leqslant 3$. The second author [20] made some conjectures for the general case. We shall now mention some special cases of (1.1) which have been treated in the literature. For more elaborate introductions, see [14] and [20].

If $P(y) \leqslant k$ in (1.1), then (1.1) asks to determine all positive integers d, k, m with $\gcd(m, d) = 1$ and $k > 2$ such that

$$P(m(m + d) \cdots (m + (k - 1)d)) \leqslant k. \tag{1.2}$$

If $d = 1$, $k = m - 1$, then Bertrand's Postulate, proved by Chebyshev, states that there are no solutions. Sylvester [18] generalised this result to all cases with $m \geqslant d + k$ and Langevin [9] to $m > k$. The authors [16] recently proved that the only solution of (1.2) with $d > 1$ is given by $m = 2$, $d = 7$, $k = 3$. If $d = 1$, $m \leqslant k$, then (1.2) is valid if and only if $\pi(k) = \pi(m + k - 1)$ which is equivalent to a well-known problem on differences between consecutive primes, see e.g. [8]. From now on we assume that $P(y) > k$.

[1]Research supported in part by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.) and by Grant #D.M.S.-8610730(1).

If $b = d = 1$, then (1.1) reduces to the problem whether the product of k consecutive positive integers can be a perfect power. Erdös [1] and Rigge [11], independently, proved that such a product can never be a square. Erdös and Selfridge [4] settled the problem completely by showing that there are no solutions at all.

Another case which has received much attention is $d = 1$, $b = k!$. Putting $n = m + k - 1$, the problem becomes to find all solutions of

$$\binom{n}{k} = y^l \tag{1.3}$$

in positive integers k, l, n, y subject to $k \geqslant 2$, $n \geqslant 2k$, $y \geqslant 2$, $l \geqslant 2$. If $k = l = 2$, then (1.3) is equivalent to the Pell equation $x^2 - 8y^2 = 1$ with $x = 2n - 1$, and it is easy to characterise the infinitely many solutions. The only other solution which is known is $n = 50$, $k = 3$, $y = 140$, $l = 2$. Erdös [1], [2] has proved that there are no solutions with $k \geqslant 4$ or $l = 3$. It follows from a result of Tijdeman [19] that there is an effectively computable upper bound for the solutions of (1.3) with $k = 2$, $l \geqslant 3$ and $k = 3$, $l \geqslant 2$.

Marszalek [10] considered equation (1.1) with $b = 1$, $d > 1$. He showed that k is bounded if d is fixed. More precisely, he proved that, for any solution of (1.1) with $b = 1$, $d > 1$, we have

$$\begin{aligned} k &\leqslant \exp(C_1 d^{3/2}) && \text{if } l = 2,\\ k &\leqslant \exp(C_2 d^{7/3}) && \text{if } l = 3,\\ k &\leqslant C_3 d^{5/2} && \text{if } l = 4,\\ k &\leqslant C_4 d && \text{if } l \geqslant 5. \end{aligned}$$

Actually he gave explicit values for the absolute constants C_1–C_4.

Shorey [14] improved on Marszalek's result. In particular Shorey [14] applied the theory of linear forms in logarithms to show that (1.1) with $l \geqslant 3$ implies that k is bounded by an effectively computable number depending only on $P(d)$.

The results in this paper considerably improve on the results of Marszalek and Shorey. As an immediate consequence of Corollary 3 and (2.7), we obtain an elementary proof of the above mentioned result of Shorey. Further, for a fixed l, we show that k is bounded if $\omega(d)$ is fixed, in particular if d is a prime number, see Corollary 3. Moreover, our results imply that for any $\varepsilon > 0$

$$k \ll_\varepsilon d^\varepsilon,$$

see Corollary 4. For k larger than some constant depending on $\omega(d)$, we even have

$$k \ll \log d,$$

see Corollary 4. In Theorem 3 we give bounds for the largest term $m + (k - 1)d$ of the arithmetical progression. Further, we notice that k is also bounded by a number depending only on m and $\omega(d)$.

2. Statements of results

If we refer to equation (1.1), we tacitly assume that the variables b, d, k, l, m, y are positive integers satisfying $P(b) \leqslant k$, $\gcd(m, d) = 1$, $k > 2$, $l > 1$, $y > 1$ and $P(y) > k$. We further assume that l is prime. By $C_5, C_6, \ldots, C_{25}$ we denote positive, effectively computable numbers. Let d_1 be the maximal divisor of d such that all the prime factors of d_1 are $\equiv 1 (\bmod\, l)$ and we set

$$d_2 = d/d_1, \qquad \theta = \max(d_2, l).$$

Notice that $d \geqslant d_1$. On the other hand, it follows from Theorem 3, formula (2.19) that

$$d_1 \geqslant C_5 d^{(l-2)/l} \quad \text{if } k \geqslant C_6, \tag{2.1}$$

where $C_5 \leqslant 1$ and C_6 are effectively computable absolute constants. This is an immediate consequence of (2.19). We write

$$h(k) = \begin{cases} \log \log k & \text{if } l \geqslant 5 \\ \log \log \log k & \text{if } l = 3 \end{cases} \tag{2.2}$$

for $k > e^e$. We start with the following result.

THEOREM 1. (a) *There exists an effectively computable absolute constant C_7 such that equation* (1.1) *with $l = 2$ implies that*

$$2^{\omega(d)} > C_7 \frac{k}{\log k}. \tag{2.3}$$

(b) *Let $\varepsilon > 0$ and $l > 3$. There exist effectively computable numbers C_8 and C_9 depending only on ε such that for every divisor d' of d satisfying*

$$d' \geqslant \begin{cases} C_8 l^{-1} \min(d^{4/l}, dk^{-l+4}) & \text{if } l \geqslant 5 \\ dk^{(-1/6)+\varepsilon} & \text{if } l = 3, \end{cases} \tag{2.4}$$

equation (1.1) *with $k \geqslant C_9$ implies that*

$$l^{\omega(d')} \geqslant (1 - \varepsilon)k \frac{h(k)}{\log k}.$$

We may apply Theorem 1(b) with $d' = 1$ to derive that

$$d \geqslant \begin{cases} C_8^{-1} k^{l-4} & \text{if } l \geqslant 5 \\ k^{(1/6)-\varepsilon} & \text{if } l = 3 \end{cases} \tag{2.5}$$

for $k \geqslant C_9$. We obtain the following sharpening of estimate (2.5).

THEOREM 2. *There exist effectively computable absolute constants* C_{10} *and* C'_{10} *such that equation* (1.1) *with* $k \geqslant C'_{10}$ *implies that*

$$d \geqslant C_{10}\theta k^{l-2}. \tag{2.6}$$

By (2.6) and $\theta \geqslant d_2$, we see that (1.1) implies that

$$d_1 \geqslant C_{10} k^{l-2} \quad \text{if } k \geqslant C'_{10}. \tag{2.7}$$

This is an improvement of a result of Shorey [14] where (2.7) reads as $d_1 > 1$ for $l \geqslant 3$ and k exceeding an effectively computable absolute constant.

Suppose that k exceeds a sufficiently large effectively computable number depending only on ε. Then, we see that (2.4) with $d' = d$ is satisfied for $l \geqslant 3$ provided that $0 < \varepsilon < 1/6$ which involves no loss of generality in the next result. Furthermore, by (2.1) and (2.7), we observe that

$$d_1 \geqslant C_8 l^{-1} d^{4/l} \quad \text{if } l \geqslant 7.$$

Therefore, the following result follows immediately from Theorem 1(b).

COROLLARY 1. *Let* $\varepsilon > 0$ *and* $l \geqslant 3$. *There exists an effectively computable number* C_{11} *depending only on* ε *such that equation* (1.1) *with* $k \geqslant C_{11}$ *implies that*

$$l^{\omega(d_1)} \geqslant (1-\varepsilon)k\frac{h(k)}{\log k} \quad \text{if } l \geqslant 7, \tag{2.8}$$

and

$$l^{\omega(d)} \geqslant (1-\varepsilon)k\frac{h(k)}{\log k} \quad \text{if } l = 3 \text{ or } l = 5. \tag{2.9}$$

So far, we have applied Theorem 1(b) for $d' = 1$, $d' = d$ and $d' = d_1$. It is useful to consider some other values of d'. For example, d has a prime power divisor $d' \geqslant d_1^{1/\omega(d_1)}$ and, by (2.1) and (2.7),

$$d' \geqslant C_5 d^{4(1+(1/l-3))/l} \geqslant C_8 l^{-1} d^{4/l} \quad \text{if } l > 4\omega(d_1) + 2.$$

Therefore, Theorem 1(b) and (2.7) admit the following consequence.

COROLLARY 2. *Let* $\varepsilon > 0$ *and*

$$l > 4\omega(d_1) + 2. \tag{2.10}$$

There exists an effectively computable number C_{12} *depending only on* ε *such that equation* (1.1) *with* $k \geqslant C_{12}$ *implies that*

$$l > (1 - \varepsilon)k \frac{\log \log k}{\log k} \tag{2.11}$$

and

$$d_1 \geqslant (\log k)^{(1-\varepsilon)k}. \tag{2.12}$$

The main aim of this paper is to prove the next two corollaries. Corollary 3 is an immediate consequence of Theorem 1(a) and Corollary 1. Corollary 4 follows from Theorem 1(a), Theorem 2 and Corollaries 1, 2.

COROLLARY 3. *Suppose that equation* (1.1) *is satisfied. If* $l \geqslant 7$, *then* k *is bounded by an effectively computable number depending only on* l *and* $\omega(d_1)$. *If* $l \in \{2, 3, 5\}$ *then* k *is bounded by an effectively computable number depending only on* $\omega(d)$.

COROLLARY 4. *Suppose that equation* (1.1) *is satisfied. Then*
(a) *there exist an effectively computable absolute constant* C_{13} *and an effectively computable number* C_{14} *depending only on* l *such that*

$$d_1 \geqslant k^{C_{13}(\log \log k)/\log \log \log k} \tag{2.13}$$

and

$$d_1 \geqslant k^{C_{14} \log \log k}. \tag{2.14}$$

(b) *Let* $\varepsilon > 0$ *and* $l \geqslant 7$. *There exists an effectively computable number* C_{15} *depending only on* ε *such that for* $k \geqslant C_{15}$ *and*

$$(4\omega(d_1) + 2)^{\omega(d_1)} < (1 - \varepsilon)k \frac{\log \log k}{\log k}, \tag{2.15}$$

we have

$$d_1 \geqslant (\log k)^{(1-\varepsilon)k}. \tag{2.16}$$

Observe that (2.14) follows immediately from (2.3), (2.8), (2.9), (2.1) and

$$\omega(d_1) \leqslant C_{16} \frac{\log d_1}{\log\log d_1}, \qquad \omega(d) \leqslant C_{16} \frac{\log d}{\log\log d} \tag{2.17}$$

where C_{16} is an effectively computable absolute constant, since $\omega(d_1) \geqslant \omega(d) - 1$ if $l = 2$. For deriving (2.13), we refer to (2.7) to assume that $l \leqslant (\log\log k)/\log\log\log k$ and then, it is a consequence of (2.14), Corollary 1 and (2.17). For Corollary 4(b), we refer to Corollary 2 to suppose that $l \leqslant 4\omega(d_1) + 2$ which, by (2.8), contradicts (2.15).

The results stated up to now do not involve m. The following result implies that if k exceeds some absolute constant, then m is bounded from above by $d^2k(\log k)^5$ if $l = 2$ and $C_{18}k\,d^{l/(l-2)}$ if $l \geqslant 3$.

THEOREM 3. *There exist effectively computable absolute constants* C_{17} *and* C_{18} *such that equation* (1.1) *with* $k \geqslant C_{17}$ *implies that*

$$m + (k-1)d \leqslant 17d^2k(\log k)^4 \quad \text{if } l = 2 \tag{2.18}$$

and

$$m + (k-1)d \leqslant C_{18}k(d\theta^{-1})^{l/(l-2)} \quad \text{if } l \geqslant 3. \tag{2.19}$$

Thus, since $\theta \geqslant d_2$, we see from (2.19) that (2.1) is valid. If k is sufficiently large and $\omega(d)$ is fixed, we refer to Corollary 3 to assume (2.10). Then, we combine $\theta \geqslant l$, (2.19) and (2.11) to derive the following result.

COROLLARY 5. *There exist effectively computable numbers* C_{19} *and* C_{20} *depending only on* $\omega(d)$ *such that equation* (1.1) *with* $k \geqslant C_{19}$ *implies that*

$$m + (k-1)d \leqslant C_{20} \frac{\log k}{\log\log k} d^{l/(l-2)}.$$

Observe that (2.19) and $\theta \geqslant l$ imply that $l^{l/(l-2)} \leqslant 2C_{18}d^{2/(l-2)}$ and consequently, we derive from (2.1) the following estimate which sharpens (2.7) if $l > k^{2+\varepsilon_1}$ for any $\varepsilon_1 > 0$.

COROLLARY 6. *There exist effectively computable absolute constants* C_{21} *and* C_{22} *such that equation* (1.1) *with* $k \geqslant C_{21}$ *implies that*

$$d_1 \geqslant (C_{22}l)^{(l-2)/2}. \tag{2.20}$$

Shorey [15] showed that there exist effectively computable absolute constants C_{23} and C_{24} such that equation (1.1) with $k \geqslant C_{23}$ implies that

$$m \geqslant d_1^{1-C_{24}\Delta_l} \quad \text{where } \Delta_l = l^{-1}(\log l)^2(\log\log(l+1)).$$

Consequently, we can find an effectively computable absolute constant C_{25} such that equation (1.1) with $l \geqslant C_{25}$ implies that k is bounded by an effectively computable number depending only on m. This assertion for equation (1.1) with $l < C_{25}$ remains unproved. We may combine this result with Corollary 3 to derive that equation (1.1) implies that k is bounded by an effectively computable number depending only on m and $\omega(d)$.

The proofs of our results are based on the following ideas. If (1.1) holds, we can write

$$m + jd = a_j x_j^l \quad (0 \leqslant j < k)$$

where each prime factor of a_j is less than k (cf. (3.2), (3.3), (4.1)). Hence

$$a_i x_i^l - a_j x_j^l = (i - j)d \quad (0 \leqslant j < i < k).$$

In the cases $l = 3$ and $l = 5$, the proofs depend on a result of Evertse [6] on the number of solutions of the diophantine equation $ax^l - by^l = c$ in positive integers x, y. In all other cases the proofs are elementary. If $a_i = a_j$ for some $i \neq j$, then

$$\begin{aligned} a_j^{1/l}(x_i - x_j)m^{(l-1)/l} &< l a_j(x_i - x_j)x_j^{l-1} < a_j(x_i^l - x_j^l) \\ &= (i - j)d < kd. \end{aligned}$$

Put $S = \{a_0, a_1, \ldots, a_{k-1}\}$. If the number $|S|$ of elements of S is relatively small, then we combine such inequalities with congruence considerations and apply the Box Principle. If $|S|$ is larger, we consider equal products of two or even four factors a_j (cf. (4.22), (4.51), (4.54)).

In §5, we shall apply p-adic theory of linear forms in logarithms to sharpen Corollary 4(b) whenever equation (1.1) with $b = 1$ is satisfied. It follows from Theorem 4 that if $b = 1$ in Corollary 4(b) then (2.16) can be replaced by the stronger inequality

$$\log d_1 \gg_\varepsilon k^2 \frac{(\log\log k)^4}{(\log k)^6} \quad \text{(cf. (5.2))}. \tag{2.21}$$

3. The case $l = 2$

We assume that b, d, k, m and y are positive integers satisfying

$$m(m + d)\cdots(m + (k - 1)d) = by^2, \tag{3.1}$$

$P(b) \leqslant k$, $\gcd(m, d) = 1$, $k > 2$ and $P(y) > k$. In the sequel $c_1, c_2, \ldots, c_7$ denote effectively computable positive absolute constants. In §3 the symbols d_1 and d_2 have another meaning than in the rest of the paper.

For $0 \leqslant i < k$, we see from (3.1) that

$$m + id = a_i x_i^2 \tag{3.2}$$

where a_i is square-free, $x_i > 0$ and $P(A_i) \leqslant k$. Further, for $0 \leqslant i < k$, we can also write

$$m + id = A_i X_i^2 \tag{3.3}$$

where

$$P(A_i) \leqslant k, \qquad X_i > 0, \qquad \gcd\left(X_i, \prod_{p \leqslant k} p \right) = 1. \tag{3.4}$$

Note that

$$\gcd(X_i, X_j) = 1 \quad \text{for } i \neq j. \tag{3.5}$$

Put

$$S = \{a_0, a_1, \ldots, a_{k-1}\} \tag{3.6}$$

and

$$S_1 = \{A_0, A_1, \ldots, A_{k-1}\}. \tag{3.7}$$

Since the left hand side of (3.1) is divisible by a prime $>k$, we have, by (3.3),

$$m + (k-1)d \geqslant (k+1)^2. \tag{3.8}$$

First, we sharpen (3.8) in the next lemma.

LEMMA 1. *Equation* (3.1) *implies that there is some effectively computable constant* $c_1 > 0$ *such that*

$$m + (k-1)d \geqslant c_1 k^3 (\log k)^2. \tag{3.9}$$

Proof. We may assume $k \geqslant c_2$ for some sufficiently large c_2 and

$$d \leqslant k^4. \tag{3.10}$$

By (3.8), we have

$$m + \mu d \geqslant k^2/4 \quad \text{for } k/4 \leqslant \mu < k. \tag{3.11}$$

We denote by T the set of all μ with $k/4 \leqslant \mu < k$ such that $X_\mu = 1$ and we write T_1 for the set of all μ with $k/4 \leqslant \mu < k$ such that $\mu \notin T$. By a fundamental argument of Erdös (cf. [5] Lemma 2.1) and (3.11), we see that

$$|T| \leqslant \frac{k \log k}{\log(k^2/4)} + \pi(k).$$

Therefore

$$|T_1| \geqslant k/8. \tag{3.12}$$

Further, notice that $X_\mu > 1$ for every $\mu \in T_1$ and hence, by (3.4) and (3.1), the numbers X_μ with $\mu \in T_1$ satisfy $X_\mu > k$ and are pairwise distinct. Further, we may suppose that X_μ is a prime number for every $\mu \in T_1$, since otherwise $m + (k-1)d \geqslant X_\mu^2 > k^4$ for some μ. Now, by (3.12), (3.3) and prime number theory, we see that there exists a subset T_2 of T_1 such that

$$|T_2| \geqslant k/16 \tag{3.13}$$

and

$$X_\mu \geqslant c_3 k \log k, \tag{3.14}$$

hence

$$m + \mu d \geqslant c_3^2 k^2 (\log k)^2 \quad \text{for } \mu \in T_2. \tag{3.15}$$

For $\mu_0 \in T_2$, we denote by $\nu(A_{\mu_0})$ the number of distinct $\mu \in T_2$ satisfying $A_\mu = A_{\mu_0}$. First, we show that

$$\nu(A_{\mu_0}) \leqslant 2^{\omega(d)+2} \quad \text{for } \mu_0 \in T_2. \tag{3.16}$$

Let $\mu_0 \in T_2$ and suppose that

$$\nu(A_{\mu_0}) > 2^{\omega(d)+2}.$$

We see from (3.3) and (3.5) that there exist $Z := 2^{\omega(d)+2}$ pairwise distinct elements $\mu_1, \ldots, \mu_z$ in T_2 distinct from μ_0 such that for $z = 1, 2, \ldots, Z$, we have $A_{\mu_0} = A_{\mu_z}$

and

$$d \mid B(\mu_0, \mu_z)B'(\mu_0, \mu_z), \qquad \gcd(B(\mu_0, \mu_z), B'(\mu_0, \mu_z)) = 1 \text{ or } 2$$

where

$$B(\mu_{z_1}, \mu_{z_2}) = |X_{\mu_{z_1}} - X_{\mu_{z_2}}|, \qquad B'(\mu_{z_1}, \mu_{z_2}) = X_{\mu_{z_1}} + X_{\mu_{z_2}}$$

for $z_1 \neq z_2$ and $0 \leqslant z_1 \leqslant Z$, $0 \leqslant z_2 \leqslant Z$. Now, we apply the Box Principle to find z_1, z_2 with $1 \leqslant z_1 < z_2 \leqslant Z$ and positive divisors d_1, d_2 of d with $d = d_1 d_2$ and $\gcd(d_1, d_2) = 1$ or 2 such that

$$d_1 | B(\mu_0, \mu_{z_1}), \; d_1 | B(\mu_0, \mu_{z_2}), \; d_2 | B'(\mu_0, \mu_{z_1}), \; d_2 | B'(\mu_0, \mu_{z_2}).$$

Consequently

$$\frac{d}{\gcd(d_1, d_2)} \Bigg| B(\mu_{z_1}, \mu_{z_2}).$$

In particular,

$$B(\mu_{z_1}, \mu_{z_2}) \geqslant \frac{d}{2}. \tag{3.17}$$

We see from (3.3) that

$$|\mu_{z_1} - \mu_{z_2}| d = A_{\mu_{z_1}} B(\mu_{z_1}, \mu_{z_2}) B'(\mu_{z_1}, \mu_{z_2})$$

which, together with (3.17), implies that

$$A_{\mu_{z_1}} B'(\mu_{z_1}, \mu_{z_2}) < 2k. \tag{3.18}$$

On the other hand, we derive from (3.3) and (3.15) that

$$A_{\mu_{z_1}} B'(\mu_{z_1}, \mu_{z_2}) \geqslant A_{\mu_{z_1}}^{1/2} (m + \mu_{z_1} d)^{1/2} \geqslant c_3 k \log k. \tag{3.19}$$

Finally, we combine (3.18) and (3.19) to arrive at a contradiction. This proves (3.16).

We denote by T_3 the set of all $\mu \in T_2$ such that

$$A_\mu > k/(2^{\omega(d)+7}) \tag{3.20}$$

and we write T_4 for the complement of T_3 in T_2. By (3.13) we observe that

$$|T_3| + |T_4| = |T_2| \geqslant k/16. \tag{3.21}$$

On the other hand, we derive from (3.16) that

$$|T_4| \leqslant k(2^{\omega(d)+2})/(2^{\omega(d)+7}) = k/32$$

which, together with (3.21), implies that

$$|T_3| \geqslant k/32. \tag{3.22}$$

We denote by S_2 the set of all $A_\mu \in S_1$ with $\mu \in T_3$ and we write S_3 for the set of all $A_\mu \in S_2$ such that $\nu(A_\mu) \geqslant 2$. We suppose that

$$|S_3| \leqslant k(64 \times 2^{\omega(d)+2})^{-1}.$$

Then, we derive from (3.22) and (3.16) that $k/32 \leqslant |T_3| \leqslant |S_2| + k/64$. Thus $|S_2| \geqslant k/64$ which, together with (3.3) and (3.14), implies (3.9).

We may therefore assume that

$$|S_3| > k(64 \times 2^{\omega(d)+2})^{-1}.$$

Then we apply the Box Principle as earlier to conclude that there exist positive divisors d_1, d_2 of d satisfying $d = d_1 d_2$, $\gcd(d_1, d_2) = 1$ or 2 and at least

$$[k(64 \times 2^{\omega(d)+2})^{-2}]$$

distinct pairs $(\mu, \nu) \in T_3^2$ such that $A_\mu = A_\nu$ and

$$X_\mu - X_\nu = r_{\mu,\nu} d_1, \qquad X_\mu + X_\nu = s_{\mu,\nu} d_2 \tag{3.23}$$

where $r_{\mu,\nu}$ and $s_{\mu,\nu}$ are positive integers satisfying

$$\max(r_{\mu,\nu}, s_{\mu,\nu}) \leqslant r_{\mu,\nu} s_{\mu,\nu} = \frac{X_\mu^2 - X_\nu^2}{d} = \frac{\mu - \nu}{A_\mu} \leqslant 2^{\omega(d)+7},$$

in view of (3.20). By (2.17) and (3.10), we have

$$[k(64 \times 2^{\omega(d)+2})^{-2}] > 2^{2\omega(d)+14}.$$

We again utilise the Box Principle to derive that there exist distinct pairs (μ_1, ν_1) and (μ_2, ν_2) such that

$$r_{\mu_1,\nu_1} = r_{\mu_2,\nu_2}, \; s_{\mu_1,\nu_1} = s_{\mu_2,\nu_2}. \tag{3.24}$$

We see from (3.23) and (3.24) that $X_{\mu_1} = X_{\mu_2}$ and $X_{\nu_1} = X_{\nu_2}$ which imply that $\mu_1 = \mu_2$ and $\nu_1 = \nu_2$. This is a contradiction. □

The following lemmas show that under suitable conditions inequality (3.9) cannot hold.

LEMMA 2. *Let S be given by* (3.6). *Suppose that a_i, a_j, a_g and a_h are elements of S satisfying*

$$a_i = a_j, \qquad a_g = a_h \tag{3.25}$$

and

$$x_i + x_j = d_1 r_1, \qquad x_i - x_j = d_2 r_2, \qquad x_g + x_h = d_1 s_1, \qquad x_g - x_h = d_2 s_2 \tag{3.26}$$

where $r_1 > 0$, $s_1 > 0$, $r_2 \neq 0$ and $s_2 \neq 0$ are integers and d_1, d_2 are positive divisors of d satisfying

$$d = d_1 d_2, \qquad \gcd(d_1, d_2) = 1 \text{ or } 2. \tag{3.27}$$

Then

$$a_i = a_g,\ r_1 = s_1 \quad \text{or} \quad a_i = a_g,\ r_2^2 = s_2^2 \quad \text{or} \quad m + (k-1)d < 272k^3.$$

Proof. There is no loss of generality in assuming that $x_i > x_j$ and $x_g > x_h$. By (3.26), we obtain

$$x_i = \frac{d_1 r_1 + d_2 r_2}{2}, \qquad x_j = \frac{d_1 r_1 - d_2 r_2}{2},$$
$$x_g = \frac{d_1 s_1 + d_2 s_2}{2}, \qquad x_h = \frac{d_1 s_1 - d_2 s_2}{2}. \tag{3.28}$$

By (3.28) and (3.2), we derive that

$$4(a_i x_i^2 - a_g x_g^2) = a_i(d_1^2 r_1^2 + 2d_1 d_2 r_1 r_2 + d_2^2 r_2^2) - a_g(d_1^2 s_1^2 + 2d_1 d_2 s_1 s_2 + d_2^2 s_2^2) \tag{3.29}$$

is divisible by d. By reading (3.29) modulo d_1 and d_2 and using (3.27), we see that

$$d_1 \mid 4(a_i r_2^2 - a_g s_2^2), \qquad d_2 \mid 4(a_i r_1^2 - a_g s_1^2) \tag{3.30}$$

which, by (3.26) and (3.27), implies that

$$dd_2 = d_1 d_2^2 \mid 4(a_i r_2^2 d_2^2 - a_g s_2^2 d_2^2) = 4(a_i(x_i - x_j)^2 - a_g(x_g - x_h)^2) \tag{3.31}$$

and

$$dd_1 = d_1^2 d_2 \mid 4(a_i r_1^2 d_1^2 - a_g s_1^2 d_1^2) = 4(a_i(x_i + x_j)^2 - a_g(x_g + x_h)^2). \tag{3.32}$$

If the right side of (3.31) vanishes, then it follows from the fact that a_i and a_g are square-free that $a_i = a_g$, $r_2^2 = s_2^2$. If the right side of (3.32) vanishes, then $a_i = a_g$, $r_1 = s_1$. Otherwise

$$a_i(x_i - x_j)^2 - a_g(x_g - x_h)^2 \neq 0, \qquad a_i(x_i + x_j)^2 - a_g(x_g + x_h)^2 \neq 0, \tag{3.33}$$

hence

$$dd_2 \leqslant 4 \max(a_i(x_i - x_j)^2, a_g(x_g - x_h)^2).$$

Without loss of generality we may assume that $a_i(x_i - x_j)^2$ is the maximal one. Then we have

$$dd_2 \leqslant 4a_i(x_i - x_j)^2 \tag{3.34}$$

and, by (3.2) and (3.25),

$$m \leqslant a_i x_j^2 \leqslant \tfrac{1}{4} a_i(x_i + x_j)^2. \tag{3.35}$$

Thus, by (3.34), (3.35), (3.25) and (3.2), $dd_2 m \leqslant (a_i x_i^2 - a_j x_j^2)^2 < k^2 d^2$. This implies

$$m < d_1 k^2. \tag{3.36}$$

From (3.32) and (3.33) we derive

$$dd_1 \mid 4((a_i x_i^2 - a_g x_g^2) + 2(a_i x_i x_j - a_g x_g x_h) + (a_i x_j^2 - a_g x_h^2)) \neq 0.$$

Since, by (3.25),

$$m \leqslant a_i x_j^2 < a_i x_i x_j < a_i x_i^2 < m + kd$$

and

$$m \leqslant a_g x_h^2 < a_g x_g x_h < a_g x_g^2 < m + kd,$$

we obtain

$$|a_i x_i x_j - a_g x_g x_h| < kd.$$

Hence $dd_1 \leqslant 16kd$. This implies that $d_1 \leqslant 16k$. Similarly, by considering (3.31) and (3.33), we obtain $d_2 \leqslant 16k$. We combine these estimates with (3.36) to conclude that $m + (k-1)d < 16k^3 + 256k^3 = 272k^3$. □

LEMMA 3. *Let* $\varepsilon > 0$ *and* S *be given by* (3.6). *There exists an effectively computable number* $C_{26} > 0$ *depending only on* ε *such that equation* (3.1) *with* $k \geqslant C_{26}$,

$$2^{\omega(d)+6} < \varepsilon \frac{k}{\log k} \tag{3.37}$$

and

$$|S| \leqslant k - \varepsilon \frac{k}{\log k} \tag{3.38}$$

implies that

$$m + (k-1)d < 272k^3. \tag{3.39}$$

Proof. Let $0 < \varepsilon < 1$. We may assume that k exceeds a sufficiently large effectively computable number depending only on ε. Observe that for every pair (i, j) with $0 \leqslant j < i < k$ and $x_i \neq x_j$, we have

$$\gcd(x_i + x_j, x_i - x_j, d) = 1 \text{ or } 2, \tag{3.40}$$

since $\gcd(m, d) = 1$. By (3.38) we conclude that the set U of pairs (i, j) with $0 \leqslant j < i < k$ and $a_i = a_j$ satisfies

$$|U| \geqslant \varepsilon \frac{k}{\log k}.$$

First, we prove the lemma with (3.37) replaced by

$$2^{3\omega(d)+9} < \varepsilon \frac{k}{\log k}.$$

We apply the Box Principle to find a subset U_1 of U satisfying

$$|U_1| \geqslant 2^{2\omega(d)+6} \tag{3.41}$$

and positive divisors d_1, d_2 of d with (3.27) such that

$$x_i + x_j = d_1 r_{i,j}, \qquad x_i - x_j = d_2 s_{i,j}, \qquad (i, j) \in U_1,$$

where $r_{i,j}$, $s_{i,j}$ are positive integers. Take an element $(i, j) \in U_1$. We argue as in the proof of (3.16), but using Lemma 1 in place of (3.15), to conclude that the number of μ with $0 \leqslant \mu < k$ satisfying $a_\mu = a_j$ is at most $2^{\omega(d)+2}$. Now, in view of (3.41), we can find a pair $(g, h) \in U_1$ such that $a_i \neq a_g$. Thus all the assumptions of Lemma 2 are satisfied and hence (3.39) is valid.

Therefore, we may assume that

$$2^{3\omega(d)+9} \geqslant \varepsilon \frac{k}{\log k}$$

which, together with (2.17), implies that

$$d \geqslant k^{C_{27} \log \log k} \tag{3.42}$$

where $C_{27} > 0$ is an effectively computable number depending only on ε. Put $\varepsilon_1 = \varepsilon/8$. Then, by (3.37) and (3.38),

$$2^{\omega(d)+3} < \varepsilon_1 \frac{k}{\log k}, \qquad |S| \leqslant k - \varepsilon_1 \frac{k}{\log k}.$$

We again apply the Box Principle to secure two distinct pairs (i, j) and (g, h) in U and positive divisors d_1, d_2 of d satisfying (3.25), (3.26) and (3.27) such that $r_2 > 0$ and $s_2 > 0$. Now, by Lemma 2, we may suppose that either

$$a_i = a_g, \qquad r_1 = s_1 \tag{3.43}$$

or

$$a_i = a_g, \qquad r_2 = s_2.$$

We give a proof for the first case and the proof for the second case is similar. Suppose $a_i = a_g$, $r_1 = s_1$. We see from (3.25) and (3.26) that $r_2 \neq s_2$. Thus, by (3.25) and (3.26),

$$x_i + x_j = x_g + x_h, \qquad x_i - x_j \neq x_g - x_h. \tag{3.44}$$

Further, observe that (3.30), (3.31) and (3.32) are valid. Then, since $r_2 < k$, $s_2 < k$, $r_2 \neq s_2$, $a_i = a_g$ and $\gcd(m, d) = 1$, we see that $\gcd(a_i, d) = 1$ and

$$d_1 < 4k^2. \tag{3.45}$$

Furthermore, by (3.43) and (3.44), the right sides of (3.31) and (3.32) are unequal and both divisible by dd_2. Therefore, by subtracting them and applying (3.43), we have $dd_2 \mid 16a_i(x_ix_j - x_gx_h) \neq 0$. Hence

$$dd_2 < 16\,|\,x_ix_j - x_gx_h|. \tag{3.46}$$

On the other hand, we see by squaring the equality in (3.44) and applying (3.43) and (3.2) that

$$2a_i|x_ix_j - x_gx_h| = |(a_ix_i^2 - a_gx_g^2) + (a_jx_j^2 - a_hx_h^2)| < 2\,dk. \tag{3.47}$$

By (3.46) and (3.47), we derive

$$d_2 < 16k \tag{3.48}$$

and therefore, by (3.45) and (3.48),

$$d = d_1d_2 < 64k^3$$

which, together with (3.42), implies that k is bounded by an effectively computable number depending only on ε. □

LEMMA 4. *Let S be given by* (3.6). *There exist effectively computable constants $c_4 > 0$ and $c_5 > 0$ such that equation* (3.1) *with*

$$|S| > k - c_4\frac{k}{\log k}$$

implies that $k \leqslant c_5$.

Proof. Let ε be an absolute constant with $0 < \varepsilon < 1$ which we choose later. We may assume that k exceeds a sufficiently large effectively computable number depending only on ε. Further, we suppose that

$$|S| > k - \varepsilon\frac{k}{\log k} =: K. \tag{3.49}$$

Then, since $a_0, \ldots, a_{k-1}$ are square-free, we derive that

$$a_0 \cdots a_{k-1} \geqslant K!(\tfrac{3}{2})^K \quad \text{(cf. [1])}. \tag{3.50}$$

We put $g_q = \operatorname{ord}_q(a_0 \cdots a_{k-1})$, $h_q = \operatorname{ord}_q(k!)$ for $q = 2, 3$. Then

$$g_q \leqslant \frac{k}{q+1} + \frac{\log k}{\log q} + 1 \quad \text{(cf. [10], p. 221)}.$$

Also,

$$h_q \geqslant \frac{k}{q-1} - \frac{\log k}{\log q} \quad \text{(cf. [10], p. 221)}.$$

Therefore

$$g_2 - h_2 \leqslant -\frac{2k}{3} + 2\frac{\log k}{\log 2} + 1, \qquad g_3 - h_3 \leqslant -\frac{k}{4} + 2\frac{\log k}{\log 3} + 1.$$

Further, by (3.2) and the fact that $P(a_i) \leqslant k$ and a_i is square free for $o \leqslant i < k$, we have

$$a_0 \cdots a_{k-1} | k! \prod_{p \leqslant k} p.$$

In fact

$$a_0 \cdots a_{k-1} \,|\, k!\, 2^{g_2 - h_2} 3^{g_3 - h_3} \prod_{p \leqslant k} p.$$

We have

$$\prod_{p \leqslant k} p \leqslant 3^k \quad \text{for } k = 1, 2, \ldots \tag{3.51}$$

(see, for example, [7]). Consequently

$$a_0 \cdots a_{k-1} \leqslant 6k^4 3^k k! 2^{-2k/3} 3^{-k/4}. \tag{3.52}$$

Now we combine (3.50), (3.52) and (3.49) to derive that

$$(\tfrac{3}{2})^k \leqslant 3^k e^{2\varepsilon k} 2^{-2k/3} 3^{-k/4} \tag{3.53}$$

for k sufficiently large. Put $\varepsilon = \frac{1}{3}\log(3^{1/4}2^{-1/3})$. Then (3.53) yields a contradiction. □

Proof of Theorem 1(*a*). We may assume that k exceeds a sufficiently large effectively computable absolute constant. Then, we derive from Lemma 4 that

$$|S| \leqslant k - c_4 \frac{k}{\log k}.$$

Assume that

$$2^{\omega(d)} < \frac{c_4}{64} \frac{k}{\log k}.$$

Then we apply Lemma 3 with $\varepsilon = c_4$ and Lemma 1 to arrive at a contradiction. □

Proof of case $l = 2$ *of Theorem* 3. We assume that (3.1) holds and

$$m > 16\, d^2 k (\log k)^4, \tag{3.54}$$

and that k exceeds a sufficiently large effectively computable absolute constant c_6. We denote by S' the set of all $a_\mu \in S$ such that $a_\mu = a_\nu$ for some $a_\nu \in S$ with $\nu \neq \mu$. Then, we observe from (3.2) and $\gcd(m, d) = 1$ that

$$a_\mu < k \quad \text{for } a_\mu \in S'. \tag{3.55}$$

For $a_{\mu_1} \in S'$ and $a_{\mu_2} \in S'$ with $\mu_1 \neq \mu_2$, we first suppose that

$$x_{\mu_1} = x_{\mu_2}. \tag{3.56}$$

Then we see from (3.2), (3.56) and $\gcd(x_{\mu_1}, d) = 1$ that

$$x_{\mu_1}^2 < k. \tag{3.57}$$

On the other hand, we derive from (3.2) and (3.55) that

$$x_{\mu_1}^2 = \frac{a_{\mu_1} x_{\mu_1}^2}{a_{\mu_1}} \geqslant mk^{-1}. \tag{3.58}$$

We combine (3.58) and (3.57) to derive that $m < k^2$ which, together with (3.54), implies that $d < k^{1/2}$. Now we apply Lemma 1 to arrive at a contradiction. Thus, we may suppose that

$$x_{\mu_1} \neq x_{\mu_2} \quad \text{for all } a_{\mu_1}, a_{\mu_2} \in S' \text{ with } \mu_1 \neq \mu_2. \tag{3.59}$$

For real numbers α, β with $0 \leqslant \alpha < \beta$ we denote by $T_{[\alpha,\beta]}$ the set of all μ with $0 \leqslant \mu < k$ such that $a_\mu \in S'$ and $k^\alpha \leqslant a_\mu < k^\beta$. We claim that

$$T_{[1-2^{1-r}, 1-2^{-r}]}| \leqslant k(\log k)^{-2} \tag{3.60}$$

for every positive integer r with

$$(2 \log k)^{2^{r+1}} \leqslant k. \tag{3.61}$$

We suppose that (3.60) does not hold for such an r and denote the corresponding set by T. Thus

$$|T| > k(\log k)^{-2}. \tag{3.62}$$

Let p be a prime number satisfying

$$\tfrac{1}{4}k^{2^{-r}}(\log k)^{-2} < p \leqslant \tfrac{1}{2}k^{2^{-r}}(\log k)^{-2}. \tag{3.63}$$

Note that such a prime exists. By (3.62) and (3.63) there exists a subset $T(p)$ of T satisfying

$$x_\mu \equiv x_\nu (\operatorname{mod} p) \quad \text{for } \mu, \nu \in T(p) \tag{3.64}$$

and

$$|T(p)| \geqslant 2k^{1-2^{-r}}. \tag{3.65}$$

Suppose that

$$a_\mu = a_\nu \quad \text{for } \mu, \nu \in T(p) \text{ with } \mu \neq \nu. \tag{3.66}$$

Then, we derive from (3.2) that

$$\mathrm{d}k > a_\mu^{1/2}|x_\mu - x_\nu| m^{1/2}. \tag{3.67}$$

By $\mu \in T$, (3.64), (3.63) and (3.54), we have

$$a_\mu^{1/2}|x_\mu - x_\nu| m^{1/2} \geqslant k^{\frac{1}{2}-2^{-r}} \cdot \tfrac{1}{4}k^{2^{-r}}(\log k)^{-2} \cdot 4\,\mathrm{d}k^{1/2}(\log k)^2. \tag{3.68}$$

Now (3.67) and (3.68) yield a contradiction. Therefore (3.66) is never valid. Consequently, by (3.65), there are at least $2k^{1-2^{-r}}$ distinct a_μ with $\mu \in T(p)$. This is impossible, since $a_\mu \leqslant k^{1-2^{-r}}$ for every such μ. Thus (3.62) is false and we have proved (3.60) for every r satisfying (3.61).

Let r_0 be the largest integer r such that (3.61) holds. Put $\delta = 2^{-r_0}$. Then

$$(2 \log k)^2 \leqslant k^\delta < (2 \log k)^4. \tag{3.69}$$

Let $\mu \in T_{[1-\delta,1]}$. Then $a_\mu = a_\nu$ for some $\nu \neq \mu$. Now, by (3.54) and (3.69),

$$\mathrm{d}k > a_\mu^{1/2}|x_\mu - x_\nu|m^{1/2} > 4k^{(1-\delta)/2}\,\mathrm{d}k^{1/2}(\log k)^2 > \mathrm{d}k,$$

a contradiction. Consequently

$$|T_{[1-\delta,1]}| = 0. \tag{3.70}$$

It further follows from the definition of r_0 that

$$r_0 < 2 \log \frac{\log k}{\log\log k} < 2\log\log k.$$

Hence, by (3.60),

$$|T_{[0,1-\delta]}| \leqslant r_0 \frac{k}{(\log k)^2} < \frac{3k\log\log k}{(\log k)^2}. \tag{3.71}$$

Combining (3.70) and (3.71), we obtain

$$|S| \geqslant k - |T_{[0,1-\delta]}| - |T_{[1-\delta,1]}| \geqslant k - c_4 \frac{k}{\log k}$$

if c_6 is sufficiently large. Now, we apply Lemma 4 to conclude that $k \leqslant c_7$. Hence, we conclude (2.18) for sufficiently large C_{17}. □

4. The case $l \geqslant 3$

For $0 \leqslant i < k$, we see from (1.1) that

$$m + id = A_i X_i^l \tag{4.1}$$

where

$$P(A_i) \leqslant k \quad \text{and} \quad \gcd\left(X_i, \prod_{p \geqslant k} p\right) = 1. \tag{4.2}$$

Note that

$$\gcd(X_i, X_j) = 1 \quad \text{for } i \neq j. \tag{4.3}$$

We put

$$S_1 = \{A_0, \ldots, A_{k-1}\}.$$

As stated in the beginning of Section 2 we assume in our results on (1.1) that $P(y) > k$. Hence, by (1.1),

$$m + (k-1)d \geqslant (k+1)^l \tag{4.4}$$

which implies that

$$m + d \geqslant k^{l-1}. \tag{4.5}$$

We recall that d_1 is the maximal divisor of d such that all the prime factors of d_1 are $\equiv 1 (\bmod l)$ and that $d_2 = d/d_1$. Let

$$d_3 = d/l^{\mathrm{ord}_l(d)}. \tag{4.6}$$

We shall follow the above notation without reference.

We first give three lemmas basically due to Erdös.

LEMMA 5. *There exists a subset S_2 of S_1 consisting of at least $|S_1| - \pi(k)$ elements such that*

$$\prod_{A_j \in S_2} A_j \leqslant k!. \tag{4.7}$$

Proof. For every prime $p \leqslant k$, we choose an $f(p) \in S_1$ such that p does not appear to a higher power in the factorisation of any other element of S_1. We denote by S_2 the set obtained by deleting these elements out of S_1. Then

$$|S_2| \geqslant k - \pi(k).$$

By counting the total contribution of prime factors $\leqslant k$ to the product of all elements of S_2, we see from (4.1) and (4.2) that

$$\prod_{A_j \in S_2} A_j \leqslant \prod_{p \leqslant k} p^{[k/p]+[k/p^2]+\cdots} = k!$$

(cf. Erdös [3] Lemma 3).

LEMMA 6. *Let $0 < \eta \leqslant \frac{1}{2}$. Let S_2 be defined as in Lemma 5. Suppose g is a positive number such that $g \leqslant (\eta \log k)/8$ and*

$$|S_2| \geqslant k - \frac{gk}{\log k}. \tag{4.8}$$

Then there exists a subset S_3 of S_2 with at least $\eta k/2$ elements satisfying

$$A_i \leqslant 4e^{(1+\eta)g}k. \tag{4.9}$$

Proof. Let S_3 be the subset of S_2 defined by (4.9). By (4.7) we have

$$k! \geqslant \prod_{A_j \in S_2} A_j \geqslant (|S_3|)!(4\,\mathrm{e}^{(1+\eta)g}k)^{|S_2|-|S_3|}.$$

Suppose $|S_3| < \eta k/2$. Then, by $n! > (n/e)^n$ for $n = 1, 2, \ldots$ and the fact that $(y/x)^y$ is monotonic decreasing in y for $0 < y < x/e$ and (4.8), we obtain

$$\begin{aligned} k! &\geqslant \left(\frac{|S_3|}{4\,\mathrm{e}^{g+\eta g+1}k}\right)^{|S_3|} (4\,\mathrm{e}^{(1+\eta)g})^{k[1-(g/\log k)]}\frac{k^k}{\mathrm{e}^{gk}} \\ &\geqslant \left(\frac{\eta}{8\,\mathrm{e}^{g+\eta g+1}}\right)^{\eta k/2}\left(\frac{4\,\mathrm{e}^{\eta g}}{(4\,\mathrm{e}^{(1+\eta)g})^{\eta/8}}\right)^{k} k^k \\ &\geqslant \left(16\left(\frac{\eta}{8e\sqrt{2}}\right)^{\eta}\right)^{k/2}\left(\frac{\mathrm{e}^{4\eta}}{\mathrm{e}^{2\eta+2\eta^2+\eta}}\right)^{gk/4} k! > k! \end{aligned}$$

which yields a contradiction. □

LEMMA 7. *Denote by $N(x)$ the maximum number of integers $1 \leqslant b_1 < b_2 < \cdots < b_u \leqslant x$ so that the products $b_i b_j$ for $1 \leqslant i \leqslant j \leqslant u$ are all distinct. For all sufficiently large x we have*

$$N(x) < 2x/\log x.$$

Proof. See Lemma 4 of Erdös [3].

By $c_8, c_9, \ldots, c_{17}$ we denote effectively computable positive absolute constants.

Proof of Theorem 2. We may assume that $l > 2$ and that $k > c_8$ where c_8 is some suitable large constant. Suppose that $A_i = A_j$, but $i > j > 0$. Then, by (4.1),

$$(i - j)d = A_j(X_i^l - X_j^l). \tag{4.10}$$

Since $\gcd(A_j, d) = 1$, we see that $A_j < k$. Further we refer to (4.1), (4.5) and (4.2) to derive that $X_i > k$ and $X_j > k$. By (4.10) and $\gcd(d, A_j) = 1$, we see that

$$d \mid (X_i^l - X_j^l).$$

We know that every prime factor of

$$(X_i^l - X_j^l)/(X_i - X_j) \tag{4.11}$$

is either l or $\equiv 1 (\bmod l)$. Further, l occurs in the factorisation of (4.11) at most to the first power. We shall use this fact several times in the paper without reference. Consequently

$$X_i - X_j \geqslant \theta l^{-1}. \tag{4.12}$$

Now, from (4.10), we derive that

$$dk > A_j^{1/l}(X_i - X_j)l(A_j X_j^l)^{(l-1)/l}. \tag{4.13}$$

If $j \geqslant k/8$, then, by (4.13), (4.12) and (4.4),

$$dk > \theta(m + jd)^{(l-1)/l} > c_9\theta(m + (k-1)d)^{(l-1)/l} > c_9\theta k^{l-1},$$

which implies that $d > c_9\theta k^{l-2}$. Thus, in the proof of Theorem 2, we may assume that the numbers A_i with $i \geqslant k/8$ are distinct. Let S_4 be the set of all integers A_i with $i \geqslant k/8$. Then $|S_4| \geqslant 7k/8$. The number of elements A_i of S_4 with $X_i = 1$ is, by (4.1), (4.5) and Lemma 5, at most

$$\pi(k) + \frac{\log k!}{(l-1)\log k} \leqslant \pi(k) + \frac{k}{2} < \frac{3k}{5}$$

for $k \geqslant c_8$. Consequently

$$|S_5| \geqslant \frac{7k}{8} - \frac{3k}{5} \geqslant \frac{k}{4} \tag{4.14}$$

for $k \geqslant c_8$ where S_5 denotes the set of elements A_i in S_4 with $X_i > 1$. Observe that, by (4.2),

$$X_i > k \quad \text{for } A_i \in S_5. \tag{4.15}$$

Consequently, by (4.1), (4.14) and (4.15), we sharpen (4.5) to

$$m + (k - 1)d \geqslant k^{l+1}/4, \tag{4.16}$$

which implies that

$$m + d \geqslant k^l/4. \tag{4.17}$$

Suppose that $A_i = A_j$ for some i, j with $i > j > 0$. Then (4.13), (4.12) and (4.17) together imply that

$$dk > \theta(m + d)^{(l-1)/l} > c_{10}\theta k^{l-1}.$$

Therefore $d > c_{10}\theta k^{l-2}$. Consequently, we may assume that $A_1, \ldots, A_{k-1}$ are distinct, hence $|S_1| \geqslant k - 1$. By applying Lemmas 5 and 6 with $\eta = \frac{1}{2}$ and $g = 2$ we obtain a subset S_3 of S_1 such that

$$|S_3| \geqslant \frac{k}{4} \tag{4.18}$$

and

$$A_i \leqslant c_{11}k \quad \text{if } A_i \in S_3. \tag{4.19}$$

Therefore, by (4.1), (4.2) and (4.17), we see that

$$X_i > k \quad \text{for } A_i \in S_3. \tag{4.20}$$

We write S_6 for the set of all $A_i \in S_3$ with $i \geqslant k/16$ and $A_i \geqslant k/16$. Then, by (4.18),

$$|S_6| \geqslant \frac{k}{8}. \tag{4.21}$$

Now, in view of (4.19) and (4.21), we can apply Lemma 7 to find elements A_i, A_j, A_μ and A_ν of S_6 satisfying

$$A_iA_j = A_\mu A_\nu \quad \text{with } i \neq \mu \quad \text{and} \quad i \neq \nu. \tag{4.22}$$

We put

$$\Delta = (m + id)(m + jd) - (m + \mu d)(m + \nu d). \tag{4.23}$$

By (4.1) and (4.22),

$$\Delta = A_\mu A_\nu((X_i X_j)^l - (X_\mu X_\nu)^l). \tag{4.24}$$

By (4.24), (4.20) and (4.3), we see that $\Delta \neq 0$. Now, there is no loss of generality in assuming that $X_i X_j > X_\mu X_\nu$. Further, we derive from (4.23), (4.24) and $\gcd(d, A_\mu A_\nu) = 1$ that

$$d \mid (X_i X_j)^l - (X_\mu X_\nu)^l.$$

Hence

$$X_i X_j - X_\mu X_\nu \geqslant \theta l^{-1}.$$

Next, observe that

$$|\Delta| \geqslant (A_\mu A_\nu)^{1/l}(X_i X_j - X_\mu X_\nu) l((A_\mu X_\mu^l)(A_\nu X_\nu^l))^{(l-1)/l}.$$

Therefore

$$|\Delta| \geqslant c_{12} k^{2/l} \theta (m + (k-1)d)^{2(l-1)/l}. \tag{4.25}$$

On the other hand, we see from (4.23) that

$$|\Delta| \leqslant 2kd(m + (k-1)d). \tag{4.26}$$

We combine (4.25) and (4.26) to obtain

$$\theta \left(\frac{m + (k-1)d}{k}\right)^{(l-2)/l} \leqslant 2c_{12}^{-1} d \tag{4.27}$$

which, together with (4.16), implies (2.6). □

Proof of case $l \geqslant 3$ of Theorem 3. We may assume that $k \geqslant c_{13}$ where c_{13} is some suitable large constant. Suppose that $A_i = A_j$ with $i > j \geqslant k/\log k$. Then, by (4.1), we see that

$$dk > (i-j)d \geqslant A_j^{1/l}(X_i - X_j) l (A_j X_j^l)^{(l-1)/l}.$$

As in the proof of (4.12) we derive that $X_i - X_j \geqslant \theta l^{-1}$. Therefore

$$\mathrm{d}k \geqslant \theta \left(\frac{m + kd}{\log k}\right)^{(l-1)/l}$$

which, together with (2.7), implies (2.19). Thus, we may assume that

$$|S_1| \geqslant k - \frac{k}{\log k}.$$

By applying Lemmas 5 and 6, we obtain a subset S'_3 of S_1 such that $|S'_3| \geqslant k/4$ and

$$A_i \leqslant c_{14}k \quad \text{for } A_i \in S'_3.$$

We now proceed as in the proof of Theorem 2 (from (4.19) on) to derive

$$\theta \left(\frac{m + (k-1)d}{k}\right)^{(l-2)/l} \leqslant c_{15}d.$$

This implies (2.19). □

In the proof of Theorem 1(b) we shall use the following lemma.

LEMMA 8. *Let* $\varepsilon > 0$. *Let* $f\colon \mathbb{R}_{>1} \to \mathbb{R}_{>1}$ *be an increasing function with* $f(x) \leqslant \log x$ for $x > 1$. *Let* d' *be a divisor of* d *satisfying*

$$d' \geqslant \begin{cases} l^{-1}(\log k)^3 \min((\mathrm{d}k)^{2/l}, \mathrm{d}k^{-l+3}) & \text{if } l \geqslant 5, \\ l^{-1}(\log k)^2 \min((\mathrm{d}k)^{2/l}, \mathrm{d}k^{(-1/3)+\varepsilon}) & \text{if } l = 3. \end{cases} \tag{4.28}$$

There exists an effectively computable number $C_{28} > 0$ *depending only on* f *and* ε *such that equation* (1.1) *with* $k \geqslant C_{28}$ *and*

$$l^{\omega(d')} < (1-\varepsilon)\frac{kf(k)}{\log k} \tag{4.29}$$

implies that

$$|S_1| \geqslant k - \left(1 - \frac{\varepsilon}{2}\right)\frac{kf(k)}{\log k}. \tag{4.30}$$

Proof. We may assume that $0 < \varepsilon < 1$ and k exceeds a sufficiently large effectively computable number depending only on f and ε. Suppose that (4.30) is not valid. We denote by S_7 the set of all $A_i \in S_1$ with $i \geqslant \varepsilon k f(k)/(4\log k)$. Then

$$|S_7| < k - \left(1 - \frac{\varepsilon}{2}\right)\frac{kf(k)}{\log k}.$$

Consequently, we can find at least $[(1-\varepsilon)kf(k)/\log k] + 1$ distinct pairs (μ, ν) with

$$k > \nu > \mu \geqslant \frac{\varepsilon k f(k)}{4\log k}, \; A_\mu = A_\nu. \tag{4.31}$$

For such a pair (μ, ν), by (4.1) and (4.31),

$$(\mu - \nu)d = A_\mu(X_\mu^l - X_\nu^l) = A_\mu \prod_{h=1}^{l} (X_\mu - \zeta^h X_\nu). \tag{4.32}$$

Since $\gcd(d, A_\mu) = 1$, we see that $A_\mu < k$. Then, by (4.1), (4.5) and (4.2), we derive that $X_\mu > k$ and $X_\nu > k$. Furthermore, by $\gcd(d, A_\mu) = 1$,

$$X_\mu^l - X_\nu^l \equiv 0 \pmod{d}, \quad \text{hence} \equiv 0 \pmod{d'}. \tag{4.33}$$

For any two such pairs (μ_1, ν_1) and (μ_2, ν_2), we say that $(X_{\mu_1}, X_{\nu_1}) \equiv (X_{\mu_2}, X_{\nu_2}) \pmod{d'}$ if

$$X_{\mu_1}X_{\nu_2} - X_{\mu_2}X_{\nu_1} \equiv 0 \pmod{d'}.$$

We denote by $R(l, d')$ the number of residue classes $z \pmod{d'}$ such that $z^l \equiv 1 \pmod{d'}$. Observe that the solutions (X_μ, X_ν) of (4.33) belong to at most $R(l, d')$ residue classes $\bmod\, d'$ and $R(l, d') \leqslant l^{\omega(d')}$. See Evertse [6, pp. 290, 294].

Therefore, it suffices to show that

$$(X_{\mu_1}, X_{\nu_1}) \not\equiv (X_{\mu_2}, X_{\nu_2}) \pmod{d'}$$

for any two distinct pairs (μ_1, ν_1) and (μ_2, ν_2) satisfying (4.31). Let (μ_1, ν_1) and (μ_2, ν_2) be distinct pairs satisfying (4.31) and

$$(X_{\mu_1}, X_{\nu_1}) \equiv (X_{\mu_2}, X_{\nu_2}) \pmod{d'}. \tag{4.34}$$

We put

$$\Delta_1 = X_{\mu_1}X_{\nu_2} - X_{\mu_2}X_{\nu_1}. \tag{4.35}$$

We see from (4.2), (4.3), (4.31) and $X_\mu > k$, $X_\nu > k$ that $\Delta_1 \neq 0$. Also observe that

$$A_{\mu_1}A_{\nu_2} = A_{\mu_2}A_{\nu_1}. \tag{4.36}$$

We put

$$\Delta_2 = (m + \mu_1 d)(m + \nu_2 d) - (m + \mu_2 d)(m + \nu_1 d). \tag{4.37}$$

Notice that $\Delta_2 \neq 0$, since $\Delta_1 \neq 0$. Further, there is no loss of generality in assuming that $X_{\mu_1}X_{\nu_2} > X_{\mu_2}X_{\nu_1}$. Now, by (4.37), (4.1) and (4.36),

$$|\Delta_2| \geqslant (A_{\mu_2}A_{\nu_1})^{1/l}|\Delta_1| l((A_{\mu_2}X_{\mu_2}^l)(A_{\nu_1}X_{\nu_1}^l))^{(l-1)/l}$$

which, together with (4.35), (4.34) and (4.31), gives

$$|\Delta_2| \geqslant d'l\left(m + \frac{\varepsilon k f(k) d}{4\log k}\right)^{2(l-1)/l} \geqslant \frac{\varepsilon^2 d' l}{16}\left(\frac{m + (k-1)d}{(\log k)/f(k)}\right)^{2(l-1)/l}. \tag{4.38}$$

On the other hand, we have

$$|\Delta_2| \leqslant 2mkd + k^2d^2 < 2kd(m + (k-1)d). \tag{4.39}$$

We combine (4.38) and (4.39) to obtain

$$((k-1)d)^{(l-2)/l} < (m + (k-1)d)^{(l-2)/l} < \frac{32}{\varepsilon^2}\frac{kd}{ld'}\left(\frac{\log k}{f(k)}\right)^{2(l-1)/l} \tag{4.40}$$

which, by (4.28) and (4.4), proves Lemma 8 for $l > 3$. If $l = 3$, then (4.40) and (4.28) imply that

$$d' \geqslant l^{-1}(\log k)^2\, dk^{-1/3+\varepsilon}.$$

Hence, by (4.40) with $l = 3$, we have

$$m + (k-1)d \leqslant \tfrac{1}{2}k^{4-3\varepsilon} \tag{4.41}$$

which implies that

$$d \leqslant k^{3-3\varepsilon}. \tag{4.42}$$

From now onward in the proof of Lemma 8, we assume that $l = 3$. We denote by T the set of all μ with $k/8 \leqslant \mu < k$ such that $X_\mu = 1$ and we write T_1 for the set of all μ with $k/8 \leqslant \mu < k$ such that $\mu \notin T$. Applying (4.4) and Lemma 5 as in the derivation of (4.14), we see that $|T| \leqslant 3k/5$ and

$$|T_1| \geqslant \frac{k}{4}.$$

By (4.41), (4.2) and (4.1), we see that

$$A_\mu < k^{1-3\varepsilon} \quad \text{for } \mu \in T_1.$$

Therefore, there exist pairwise distinct elements $\mu_0, \ldots, \mu_Z \in T_1$ with $Z = [k^{2\varepsilon}]$ such that

$$A_{\mu_0} = A_{\mu_1} = \cdots = A_{\mu_Z}.$$

By (2.17) and (4.42), we may assume that

$$Z > 9^{\omega(d)}.$$

We write

$$\zeta = e^{2\pi i/l}, \qquad K = \mathbb{Q}(\zeta).$$

We denote by Σ_K the ring of algebraic integers of K and we write D_K for the discriminant of K. We know

$$[K:\mathbb{Q}] = l-1, \qquad |D_K| = l^{l-2}.$$

For $v \in \Sigma_K$, we denote by $[v]$ the principal ideal generated by v in Σ_K. Now we use the Box Principle to find μ_i and μ_j with $i \neq j$ and pairwise coprime ideals $\mathscr{D}_1$, $\mathscr{D}_2$, $\mathscr{D}_3$ satisfying

$$[d_3] = \mathscr{D}_1\mathscr{D}_2\mathscr{D}_3$$

where

$$d_3 = d/3^{\operatorname{ord}_3(d)}$$

and

$$\mathscr{D}_h \mid [X_{\mu_0} - \zeta^h X_{\mu_i}], \qquad \mathscr{D}_h \mid [X_{\mu_0} - \zeta^h X_{\mu_j}] \quad \text{for } h = 1, 2, 3. \tag{4.43}$$

We put

$$\Delta_1' = X_{\mu_i} - X_{\mu_j} \neq 0.$$

Then, by (4.33),

$$d \mid (X_{\mu_i}^3 - X_{\mu_j}^3), \quad \text{but } 9 \nmid (X_{\mu_i}^3 - X_{\mu_j}^3)/\Delta_1'$$

so that

$$3^{\operatorname{ord}_3(d)-1} \mid \Delta_1' \quad \text{if } \operatorname{ord}_3(d) > 0.$$

Also, by (4.43),

$$d_3 \mid \Delta_1'.$$

Hence

$$d \leqslant 3|\Delta_1'|. \tag{4.44}$$

There is no loss of generality in assuming that $X_{\mu_i} > X_{\mu_j}$. Since $A_{\mu_i} = A_{\mu_j}$, we see from (4.1) that

$$dk > 3A_{\mu_j}^{1/3}\Delta_1'(A_{\mu_j}X_{\mu_j}^3)^{2/3}$$

which, together with (4.44) and (4.4), implies that

$$k > c_{17}(m + (k-1)d)^{2/3} > c_{17}k^2.$$

This is a contradiction.

Proof of Theorem 1(*b*). We may assume that $0 < \varepsilon < 1$. We denote by C_{29}, $C_{30}, \ldots, C_{38}$ effectively computable positive numbers depending only on ε. We may suppose that k exceeds a sufficiently large effectively computable number depending only on ε. Further we assume that

$$l^{\omega(d')} < (1-\varepsilon)\frac{kh(k)}{\log k}. \tag{4.45}$$

Observe that (2.4) implies (4.28) by (2.7). Then by Lemma 8,

$$|S_1| \geqslant k - \left(1 - \frac{\varepsilon}{2}\right)\frac{kh(k)}{\log k}.$$

Now, the set S_2 of Lemma 5 satisfies

$$|S_2| \geqslant k - \left(1 - \frac{\varepsilon}{3}\right) \frac{kh(k)}{\log k} =: t.$$

By Lemma 6 with $\eta = \varepsilon/13$ and $g = (1 - \varepsilon/3)\, h(k)$, there exists a subset S_8 of S_2 such that

$$|S_8| \geqslant \frac{\varepsilon k}{26} \tag{4.46}$$

and

$$A_i \leqslant 4\,\mathrm{e}^{(1+\varepsilon/13)(1-\varepsilon/3)h(k)} k \leqslant k\,\mathrm{e}^{(1-\varepsilon/4)h(k)} \quad \text{if } A_i \in S_8. \tag{4.47}$$

Thus, by (4.5) and (4.2),

$$X_i > k \quad \text{if } A_i \in S_8. \tag{4.48}$$

Now we derive from (4.1), (4.46) and (4.48) that

$$m + (k-1)d \geqslant C_{29} k^{l+1}. \tag{4.49}$$

First assume $l \geqslant 5$. Denote by S_9 the set of all $A_i \in S_8$ with $i \geqslant \varepsilon k/104$ and $A_i \geqslant \varepsilon k/104$. Then, we see from (4.46) that $|S_9| \geqslant \varepsilon k/52$. Denote by S_{10} a maximal subset of S_9 such that all products $A_i A_j$ with A_i, $A_j \in S_{10}$ are distinct. Then, by Lemma 7 and (4.47),

$$|S_{10}| \leqslant \frac{2k\,\mathrm{e}^{(1-\varepsilon/4)h(k)}}{\log k} = \frac{2k}{(\log k)^{\varepsilon/4}}.$$

We write S_{11} for the complement of S_{10} in S_9. Then

$$|S_{11}| \geqslant \frac{\varepsilon k}{53}. \tag{4.50}$$

For every $A_\nu \in S_{11}$ there exist elements A_{i_ν}, A_{j_ν} and A_{μ_ν} in S_{10} satisfying

$$A_{i_\nu} A_{j_\nu} = A_{\mu_\nu} A_\nu \tag{4.51}$$

by the definitions of S_{10} and S_{11}. By (4.1) and (4.51), we see that

$$d' \mid (X_{i_\nu} X_{j_\nu})^l - (X_{\mu_\nu} X_\nu)^l.$$

By (4.3) and (4.48), we observe that $X_{i_\nu} X_{j_\nu} \neq X_{\mu_\nu} X_\nu$. Now, we proceed as in the proof of Lemma 8 to derive from (4.45) and (4.50) that we may assume that

$$\Delta_3 \equiv 0 \pmod{d'} \tag{4.52}$$

where

$$\Delta_3 = X_{i_{\nu_1}} X_{j_{\nu_1}} X_{\mu_{\nu_2}} X_{\nu_2} - X_{i_{\nu_2}} X_{j_{\nu_2}} X_{\mu_{\nu_1}} X_{\nu_1}$$

for distinct integers ν_1, ν_2 with $A_{\nu_\delta} \in S_{11}$, $A_{i_{\nu_\delta}} \in S_{10}$, $A_{j_{\nu_\delta}} \in S_{10}$ and $A_{\mu_{\nu_\delta}} \in S_{10}$ satisfying

$$A_{i_{\nu_\delta}} A_{j_{\nu_\delta}} = A_{\mu_{\nu_\delta}} A_{\nu_\delta} \quad \text{for } \delta = 1, 2. \tag{4.53}$$

By (4.3) and (4.48), we see that $\Delta_3 \neq 0$. Then there is no loss of generality in assuming that $\Delta_3 > 0$. By (4.53), we derive that

$$A_{i_{\nu_1}} A_{j_{\nu_1}} A_{\mu_{\nu_2}} A_{\nu_2} = A_{i_{\nu_2}} A_{j_{\nu_2}} A_{\mu_{\nu_1}} A_{\nu_1}. \tag{4.54}$$

We put

$$\begin{aligned} \Delta_4 = {} & (m + i_{\nu_1} d)(m + j_{\nu_1} d)(m + \mu_{\nu_2} d)(m + \nu_2 d) \\ & -(m + i_{\nu_2} d)(m + j_{\nu_2} d)(m + \mu_{\nu_1} d)(m + \nu_1 d). \end{aligned} \tag{4.55}$$

By (4.1), (4.55), (4.54) and $\Delta_3 > 0$, we observe that

$$\Delta_4 > C_{30}(A_{i_{\nu_2}} A_{j_{\nu_2}} A_{\mu_{\nu_1}} A_{\nu_1})^{1/l} \Delta_3 l (m + (k-1)d)^{4(l-1)/l}.$$

Now we apply (4.52) to derive that

$$\Delta_4 > C_{31} k^{4/l} d' l (m + (k-1)d)^{4(l-1)/l}. \tag{4.56}$$

On the other hand, we see from (4.55) that

$$\Delta_4 < 4kd(m + (k-1)d)^3. \tag{4.57}$$

We combine (4.56) and (4.57) to obtain

$$d^{(l-4)/l} < 2\left(\frac{m + (k-1)d}{k}\right)^{(l-4)/l} < C_{32} \frac{d}{ld'},$$

which, by $l \geqslant 5$, (2.4) and (4.49), is not possible if C_8 if sufficiently large.

It remains to consider the case $l = 3$. Recall that we have a subset S_8 of S_1 satisfying (4.46) – (4.48). Denote by S_{12} the set of all $A_i \in S_8$ such that $A_i \geqslant k/(\log k)^{1/8}$. Then

$$|S_{12}| \geqslant \frac{\varepsilon k}{26} - \frac{k}{(\log k)^{1/8}} \geqslant \frac{\varepsilon k}{27}. \tag{4.58}$$

Denote by $b_1, b_2, \ldots, b_s$ all integers between $k/(\log k)^{1/8}$ and $k(\log\log k)^{1-\varepsilon/4}$ such that every proper divisor of b_i is less than or equal to $k/(\log k)^{1/8}$. If $b_i > k/(\log k)^{1/16}$, then every prime divisor of b_i exceeds $(\log k)^{1/16}$. By Brun's sieve

$$s \leqslant \frac{k}{(\log k)^{1/16}} + C_{33}\frac{k}{(\log\log k)^{\varepsilon/4}} < \frac{k}{(\log\log k)^{\varepsilon/5}}.$$

By (4.47) every element of S_{12} is divisible by at least one b_i. Denote by S_{13} the subset of S_{12} consisting of A_i corresponding to b_i which appear in at most one element of S_{12}. Then

$$|S_{13}| \leqslant s \leqslant k(\log\log k)^{-\varepsilon/5}.$$

Denote by S_{14} the complement of S_{13} in S_{12}. Then, by (4.58),

$$|S_{14}| \geqslant \frac{\varepsilon k}{30}$$

and

$$\gcd(A_\mu, A_\nu) \geqslant \frac{k}{(\log k)^{1/8}}, \; \mu \neq \nu, \quad A_\mu, A_\nu \in S_{14} \tag{4.59}$$

is satisfied by at least $\varepsilon k/60$ distinct pairs A_μ, A_ν.

Let A_μ, A_ν be a pair satisfying (4.59). We have, by (4.1), (4.47) and (4.59),

$$LX_\mu^3 - MX_\nu^3 = Nd$$

where

$$L = \frac{A_\mu}{\gcd(A_\mu, A_\nu)}, \qquad M = \frac{A_\nu}{\gcd(A_\mu, A_\nu)}, \qquad N = \frac{\mu - \nu}{\gcd(A_\mu, A_\nu)}$$

and

$$\max(L, M, N) \leqslant (\log k)^{1/4}.$$

By the Box Principle we find coprime positive integers L_1, M_1, N_1 such that

$$\max(L_1, M_1, N_1) \leqslant (\log k)^{1/4} \tag{4.60}$$

and

$$L_1 X_\mu^3 - M_1 X_\nu^3 = N_1 d =: N_2 d'$$

is valid for at least $\varepsilon k/(60(\log k)^{3/4})$ distinct pairs X_μ, X_ν. By (2.4), (4.60) and (2.7), we have

$$N_2 \leqslant (d')^{1/5}.$$

Hence we obtain, by applying Evertse [6] Corollary 1(ii),

$$\frac{\varepsilon k}{60(\log k)^{3/4}} \leqslant 4 \cdot 3^{\omega(d')} + 3$$

which, by (4.45), is not possible if k is sufficiently large. □

5. The case $b = 1$

If every $m + \mu d$ with $0 \leqslant \mu < k$ is an l-th perfect power, then Shorey and Tijdeman [17] showed that

$$\log d \geqslant c_{18} k^2$$

where $c_{18} > 0$ is an effectively computable absolute constant. Here we consider the weaker condition $b = 1$ and we prove:

THEOREM 4. *Let $\varepsilon > 0$ and $l \geqslant 7$. There exist effectively computable numbers C_{34} and $C_{35} > 0$ depending only on ε such that equation* (1.1) *with $b = 1$, $k \geqslant C_{34}$ and*

$$(4\omega(d) + 2)^{\omega(d)} < (1 - \varepsilon)k \frac{\log\log k}{\log k} \tag{5.1}$$

implies that

$$\log d_1 \geqslant C_{35} k^2 \frac{(\log\log k)^4}{(\log k)^6}. \tag{5.2}$$

The proof of Theorem 4 depends on the following result which is more general than we require.

LEMMA 9. *Let* $0 < \phi \leqslant 1$. *Assume that there exists a prime* p *satisfying* $\gcd(p, d) = 1$, $p \neq l$,

$$2k^{1-\phi}\left(\frac{\log k}{\log\log k}\right)^{\phi} \leqslant p < 2k^{1-\phi}(\log k)^{\phi} \tag{5.3}$$

and

$$\mathrm{ord}_p(m(m+d)\cdots(m+(k-1)d)) \geqslant l^{\phi}. \tag{5.4}$$

There exist effectively computable numbers C_{36}, C_{37} *and* $C_{38} > 0$ *depending only on* ϕ *such that equation* (1.1) *with* $k \geqslant C_{36}$ *and* (2.10) *implies that*

$$l^{1+\phi} \leqslant C_{37}(\log\log k)^{-2}(\log k)^{1+2\phi}k^{2-2\phi}(\log \mathrm{d}_1)(\log\log d_1) \tag{5.5}$$

and

$$\log d_1 \geqslant C_{38}k^{3\phi-1}\frac{(\log\log k)^{3+\phi}}{(\log k)^{3+3\phi}}. \tag{5.6}$$

First, we assume Lemma 9 and we proceed to derive Theorem 4. Suppose that equation (1.1) with $b = 1$ and (5.1) is valid. Then, by Prime number theory, we see from (5.1) that there is a prime p satisfying $\gcd(p, d) = 1$, $p \neq l$ and (5.3) with $\phi = 1$ if $k \geqslant C_{34}$ with C_{34} sufficiently large. Furthermore, since $b = 1$, inequality (5.4) with $\phi = 1$ is valid. Also, by (2.8), we notice that (5.1) implies $l > 4\omega(d) + 2 \geqslant 4\omega(d_1) + 2$. Finally, we apply Lemma 9 with $\phi = 1$ to conclude (5.2). Therefore, it remains to prove Lemma 9.

Proof of Lemma 9. We denote by C_{39}, C_{40}, and C_{41} effectively computable positive numbers depending only on ϕ. We may assume that $k \geqslant C_{39}$ with C_{39} sufficiently large. Let μ_0 with $0 \leqslant \mu_0 < k$ satisfy

$$0 < \mathrm{ord}_p(m + \mu_0 d) = \max_{0 \leqslant i < k} \mathrm{ord}_p(m + id). \tag{5.7}$$

By Lemma 5, we can find μ_1 and μ_2 with $0 \leqslant \mu_1 < k$, $0 \leqslant \mu_2 < k$ such that μ_0, μ_1, μ_2 are pairwise distinct and

$$A_{\mu_i} \leqslant k^2, \qquad i = 1, 2. \tag{5.8}$$

We have

$$(\mu_1 - \mu_2)(m + \mu_0 d) = -(\mu_2 - \mu_0)(m + \mu_1 d) - (\mu_0 - \mu_1)(m + \mu_2 d). \tag{5.9}$$

By (5.9) and (4.1),

$$\operatorname{ord}_p(m + \mu_0 d) \leqslant \operatorname{ord}_p(B_1 X_{\mu_1}^l - B_2 X_{\mu_2}^l) \tag{5.10}$$

where

$$B_1 = -(\mu_2 - \mu_0)A_{\mu_1}, \qquad B_2 = (\mu_0 - \mu_1)A_{\mu_2}. \tag{5.11}$$

Further, we notice from (5.11) and (5.8) that

$$|B_i| < k^3,\ \operatorname{ord}_p(B_i) \leqslant 6\frac{\log k}{\log p}, \qquad i = 1, 2. \tag{5.12}$$

Consequently, by (5.7), (5.10), (5.12) and (4.2),

$$0 < \operatorname{ord}_p(m + \mu_0 d) \leqslant \operatorname{ord}_p\left(\frac{B_1}{B_2}\left(\frac{X_{\mu_1}}{X_{\mu_2}}\right)^l - 1\right) + \frac{6\log k}{\log p}. \tag{5.13}$$

Now, we apply a result of Yu [22] on p-adic linear forms in logarithms to derive from (5.12), (5.3) and (4.1) that

$$\begin{aligned}\operatorname{ord}_p\left(\frac{B_1}{B_2}\left(\frac{X_{\mu_1}}{X_{\mu_2}}\right)^l - 1\right) &\leqslant C_{40}\frac{(\log k)^{1+2\phi}k^{2-2\phi}(\log l)\log(m + (k-1)d)}{l(\log\log k)^2} \\ &\leqslant C_{41}\frac{(\log k)^{1+2\phi}k^{2-2\phi}(\log l)(\log d_1)}{l(\log\log k)^2}\end{aligned} \tag{5.14}$$

by (2.19) with $\theta \geqslant d_2$ and (2.7). Further, we observe that

$$\begin{aligned}\operatorname{ord}_p(m(m+d)\cdots(m+(k-1)d)) &\leqslant \operatorname{ord}_p(m + \mu_0 d) + \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots \\ &\leqslant \operatorname{ord}_p(m + \mu_0 d) + \frac{k}{p-1}\end{aligned}$$

which, together with (5.4), implies that

$$l^\phi \leqslant \operatorname{ord}_p(m + \mu_0 d) + \frac{k}{p-1}. \tag{5.15}$$

Now, we apply (5.3) and (2.11) to derive that

$$\frac{k}{p-1} + 6\frac{\log k}{\log p} \leqslant \frac{2}{3}k^{\phi}\left(\frac{\log\log k}{\log k}\right)^{\phi} \leqslant \frac{3}{4}l^{\phi}. \tag{5.16}$$

Therefore, by (5.15), (5.13), (5.16) and (5.14), we have

$$l^{1+\phi} \leqslant 4C_{41}\frac{(\log k)^{1+2\phi}k^{2-2\phi}}{(\log\log k)^2}(\log l)(\log d_1)$$

which, together with (2.12), implies (5.5). Finally, we combine (2.11) and (5.5) to obtain (5.6). □

REMARKS. The proof of Theorem 1 for $l \neq 3$ is entirely elementary. In the case $l = 3$, we use a result of Evertse. By using an elementary argument, we can prove, instead of (2.9) with $l = 3$, that there is an effectively computable absolute constant $c_{18} > 0$ such that

$$3^{\omega(d)} > c_{18}k^{1/6}.$$

(ii) The arguments of the proof of Theorem 1 are valid for the more general equation

$$(m + d_1 d)\cdots(m + d_t d) = by^l \tag{5.17}$$

where $d_1, \ldots, d_t$ are distinct integers between 1 and k. In particular, we have: *for every $\varepsilon > 0$ there exist effectively computable numbers C_{42} and C_{43} depending only on ε such that equation* (5.17) *with $k \geqslant C_{42}$ and*

$$t \geqslant k - C_{43}k\frac{H(k)}{\log k}$$

implies (2.7), (2.8) *and* (2.9), *where $H(k) = h(k)$ if $l \geqslant 3$ and $H(k) = 1$ if $l = 2$.* Much better results have been proved by Shorey [12], [13] for equation (5.17) with $d = 1$ via the theory of linear forms in logarithms and irrationality measures of Baker proved by the hypergeometric method.

(iii) By applying an idea of [12, Lemma 6], it is possible to give a proof of Theorem 4 where we require only the estimates on p-adic linear forms in logarithms with an independence (Kummer) condition. Thus, the results of [21] are sufficient for the proof of Theorem 4.

References

1. P. Erdös, *Note on the product of consecutive integers* (I) and (II), *J. London Math. Soc.* 14 (1939), 194–198 and 245–249.
2. P. Erdös, On a diophantine equation, *J. London Math. Soc.* 26 (1951), 176–178.
3. P. Erdös, On the product of consecutive integers III, *Indag. Math.* 17 (1955), 85–90.
4. P. Erdös and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* 19 (1975), 292–301.
5. P. Erdös and J. Turk, Products of integers in short intervals, *Acta Arith.* 44 (1984), 147–174.
6. J.-H. Evertse, On the equation $ax^n - by^n = c$, *Compositio Math.* 47 (1982), 289–315.
7. D. Hanson, On a theorem of Sylvester and Schur, *Canad. Math. Bull.* 16 (1973), 195–199.
8. H. Iwaniec and J. Pintz, Primes in short intervals, *Monatsh. Math.* 98 (1984), 115–143.
9. M. Langevin, Plus grand facteur premier d'entiers en progression arithmétique, Sém. Delange-Pisot-Poitou, 18e année, 1976–77, no. 3, 7 pp.
10. R. Marszalek, On the product of consecutive elements of an arithmetic progression, *Monatsh. Math.* 100 (1985), 215–222.
11. O. Rigge, *Über ein diophantisches Problem*, 9th Congress Math. Scand., Helsingfors, 1938, Mercator, Helsingfors, 1939, 155–160.
12. T. N. Shorey, Perfect powers in values of certain polynomials at integer points, *Math. Proc. Camb. Phil. Soc.* 99 (1986), 195–207.
13. T. N. Shorey, Perfect powers in products of integers from a block of consecutive integers, *Acta Arith.* 49 (1987), 71–79.
14. T. N. Shorey, Some exponential diophantine equations, New Advances in Transcendence Theory, ed. by A. Baker, Cambridge University Press, 1988, pp. 352–365.
15. T. N. Shorey, *Some exponential diophantine equations* II, Number Theory and Related Topics, Tata Institute of Fundamental Research, Bombay, 1988, pp. 217–229.
16. T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression*, A Tribute to Paul Erdös, Cambridge Univ. Press, to appear.
17. T. N. Shorey and R. Tijdeman, *Perfect powers in arithmetical progression*, J. Madras Univ., Section B, 51 (1988), 173–180.
18. J. J. Sylvester, On arithmetic series, *Messenger Math.* 21 (1892), 1–19 and 87–120.
19. R. Tijdeman, *Applications of the Gel'fond-Baker method to rational number theory*, Coll. Math. Jańos Bolyai, 13. Topics in Number Theory (Debrecen, 1974), North-Holland, Amsterdam, 1976, pp. 399–416.
20. R. Tijdeman, *Diophantine equation and diophantine approximations*, Number Theory and Applications, Kluwer Acad. Publ., Dordrecht, 1989, pp. 215–243.
21. Kunrui Yu, Linear forms in the p-adic logarithms, *Acta. Arith.* 53 (1989), 107–186.
22. Kunrui Yu, Linear forms in p-adic logarithms II, *Compositio Math.* 74 (1990), 15–113.