ACTA ARITHMETICA
LXI.4 (1992)

Perfect powers in products of terms in an arithmetical progression III

by

T. N. Shorey (Bombay) and R. Tijdeman (Leiden)

1. 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 $\omega(1) = 0$. Let $d \geq 1$, $k \geq 2$ and $m \geq 0$ be integers such that $\gcd(m, d) = 1$. Let $d_1, \ldots, d_t$ with $t \geq 2$ be distinct integers in the interval $[0, k)$. For integers $l \geq 2, y > 0$ and $b > 0$ with $P(b) \leq k$, we consider the equation

$$(m + d_1 d) \ldots (m + d_t d) = by^l. \tag{1}$$

If $P(y) \leq k$, it follows from an argument of Erdős (see [3, Lemma 2.1]) that (1) implies that

$$t - 1 \leq \frac{k \log k}{\log(m + d)}.$$

Now onward whenever we refer to equation (1), we always assume that the left-hand side of (1) has a prime factor $> k$ and thus

$$\chi =: m + (k - 1)d \geq (k + 1)^l. \tag{2}$$

Further, we write

$$\Delta(m, k, d) = m(m + d) \ldots (m + (k - 1)d).$$

We shall follow this notation without reference. For an account of results on equation (1), we refer to Shorey [9], Shorey and Tijdeman [12].

First, we consider equation (1) with $d = 1$ which, by (2), implies that $m > k^l$. Erdős [2], p. 88, showed that for $\varepsilon > 0$ there exists an effectively computable number C depending only on ε such that equation (1) with $b = 1, d = 1, l > 2$ and $k \geq C$ implies that

$$t \leq k - (1 - \varepsilon)k \frac{\log \log k}{\log k}. \tag{3}$$

Further, Erdős [1], [2], p. 88, showed that there exist effectively computable absolute constants C_1 and $C_2 > 0$ such that equation (1) with $b = 1$, $d = 1$,

$l = 2$ and $k \geq C_1$ implies that

$$t \leq k - C_2 k/\log k. \tag{4}$$

See Erdős and Turk [3] for some extensions of these results. The proofs of these results are elementary. Shorey [7, 8] combined this elementary method of Erdős with the theory of linear forms in logarithms, irrationality measures of Baker on the approximations of certain algebraic numbers by rationals and the method of Roth–Halberstam on μ-free integers to sharpen (3) considerably. It has been proved in [7, 8] that there exists an effectively computable absolute constant C_3 such that equation (1) with $d = 1, l > 2$ and $k \geq C_3$ implies that

$$t \leq \nu_l k \quad \text{with} \quad \nu_l = \frac{1}{2}\left(1 + \frac{4l^2 - 8l + 7}{2(l-1)(2l^2 - 5l + 4)}\right). \tag{5}$$

We observe that

$$\nu_3 = \frac{47}{56}, \quad \nu_4 = \frac{45}{64} \quad \text{and} \quad \nu_l \leq \frac{299}{464} < \frac{2}{3} \quad \text{for } l \geq 5.$$

If l is sufficiently large, estimate (5) can be sharpened. Shorey [7] applied the theory of linear forms in logarithms to prove that there exists an effectively computable absolute constant C_4 such that equation (1) with $d = 1$, $l \geq C_4$ and $k \geq C_4$ implies that

$$t \leq k l^{-1/11} + \pi(k) + 2. \tag{6}$$

For $l = 2$, Erdős [2], p. 88, asked whether (4) can be replaced by (3). Shorey [8] combined the method of Erdős with a theorem of Baker on the finiteness of integer solutions of the hyper-elliptic equation to show that this is, in fact, the case. More precisely, it has been shown in [7, 8] that given $\varepsilon > 0$ there exists an effectively computable number C_5 depending only on ε such that equation (1) with $d = 1$, $l = 2$ and $k \geq C_5$ implies (3). As a consequence of these results, we shall derive

Theorem 1. *Let $\varepsilon > 0$ and $m + k - 1 > k^l$. There exists an effectively computable number C_6 depending only on ε such that for $k \geq C_6$ we can find a prime p with*

$$0 < \operatorname{ord}_p(\Delta(m,k,1)) \not\equiv 0 \pmod{l}$$

such that

$$p \geq \begin{cases} (1-\varepsilon)k \log\log k & \text{if } l = 2\,, \\ (1-\nu_l-\varepsilon)k\log k & \text{if } l > 2\,, \\ (1-\varepsilon)k\log k & \text{if } l > C_6\,. \end{cases}$$

If $m \leq k^l$, we observe that $\operatorname{ord}_p(\Delta(m,k,1)) \not\equiv 0 \pmod{l}$ for every prime $p > k$ such that $p \mid \Delta(m,k,1)$. Therefore, it suffices to consider lower bounds for $P(\Delta(m,k,1))$ to obtain an analogue of Theorem 1 in the case $m \le k^l$. For this, we refer to Shorey [6] and Shorey and Tijdeman [10], Chapter 7.

Next, we consider (1) with $d > 1$. There is no loss of generality in assuming that l is a prime number. We put

$$h(k) = \begin{cases} \log\log k & \text{if } l \ge 5, \\ \log\log\log k & \text{if } l = 3, \end{cases}$$

for $k > e^e$. We obtain the following weaker analogue of the above stated results of Shorey.

THEOREM 2. (a) *Let $\varepsilon > 0$. There exists an effectively computable number C_7 depending only on ε and $\omega(d)$ such that equation* (1) *with $l = 2$ and $k \ge C_7$ implies that*

$$t \le k - (1-\varepsilon)k\frac{\log\log\log k}{\log k}. \tag{7}$$

(b) *Let $\varepsilon > 0$ and $l > 2$ be a prime number. There exist effectively computable numbers C_8 and C_9 depending only on ε such that equation* (1) *with $k \ge C_8$ and*

$$l^{\omega(d)} \le C_9 k\frac{h(k)}{\log k} \tag{8}$$

implies that

$$t \le k - (1-\varepsilon)k\frac{h(k)}{\log k}.$$

Theorem 2 with $t = k$ is contained in Shorey and Tijdeman [12], Theorem 1. The proof of Theorem 2(a) depends on Brun's Sieve and a theorem of Evertse and Silverman [5] on the number of integer solutions of the hyperelliptic equation. The proof of Theorem 2(b) with $l \ge 5$ is elementary and we apply a theorem of Evertse [4] in the case $l = 3$. We apply Theorem 2 to derive the following analogue of Theorem 1 for $\Delta(m,k,d)$.

COROLLARY 1. *Let $\varepsilon > 0$ and $\chi > k^l$.*

(a) *There exists a prime p dividing $\Delta(m,k,d)$ such that*

$$p \ge (1-\varepsilon)k\log\log\log k \quad \textit{and} \quad \mathrm{ord}_p(\Delta(m,k,d)) \not\equiv 0 \pmod 2$$

whenever k exceeds an effectively computable number depending only on ε and $\omega(d)$.

(b) *Let $l > 2$ be a prime number. There exist effectively computable numbers C_{10} and C_{11} depending only on ε such that for $k \ge C_{10}$ and*

$$l^{\omega(d)} \le C_{11} k\frac{h(k)}{\log k}, \tag{9}$$

we can find a prime p dividing $\Delta(m,k,d)$ satisfying

$$p \ge (1-\varepsilon)kh(k) \quad \textit{and} \quad \mathrm{ord}_p(\Delta(m,k,d)) \not\equiv 0 \pmod{l}.$$

For an analogue of Corollary 1 in the case $\chi \le k^l$, it is equivalent to considering lower bounds for $P(\Delta(m,k,d))$. We refer to Shorey and Tijdeman [11, 13] for these bounds. We write

$$h'(k) = \begin{cases} h(k) & \text{if } l \ge 3, \\ \log\log\log k & \text{if } l = 2. \end{cases}$$

The following result is a particular case of Corollary 1 whenever l and $\omega(d)$ are bounded.

Corollary 2. *Let $l \ge 2$ be a prime number. Let $\varepsilon > 0$ and $\chi > k^l$. There exists a prime p dividing $\Delta(m,k,d)$ such that*

$$p \ge (1-\varepsilon)kh'(k) \quad \textit{and} \quad \mathrm{ord}_p(\Delta(m,k,d)) \not\equiv 0 \pmod{l}$$

whenever k exceeds an effectively computable number depending only on ε, l and $\omega(d)$.

2. Proof of Theorem 2. (a) Let $c > 0$ be a number depending only on ε and $\omega(d)$. We shall choose c later. We may assume that k exceeds a sufficiently large effectively computable number depending only on ε, c and $\omega(d)$. For $1 \le i \le t$, we see from (1) that

$$m + d_i d = a_i x_i^2 \tag{10}$$

where a_i is square-free such that $P(a_i) \le k$ and x_i is a positive integer. Let S be the set of all a_i with $1 \le i \le t$ such that $d_i > 0$. We may suppose that

$$t \ge k - (1-\varepsilon)k\frac{\log\log\log k}{\log k}. \tag{11}$$

Then, we argue as in the proof of Lemma 1 of [12] to derive that

$$\chi \ge c_2 k^3 (\log k)^2. \tag{12}$$

Further, we refer to the proof of Lemma 3 of [12] to conclude from (11) and (12) that

$$|S| \ge k - \left(1 - \frac{3\varepsilon}{4}\right) k \frac{\log\log\log k}{\log k}. \tag{13}$$

Next, we follow the proof of Theorem 2 of [7] without reference. By (13), there exists a subset S_1' of S such that $|S_1'| \ge \varepsilon k/2$ and

$$a_i \le k(\log\log k)^{1-\varepsilon/2} \quad \text{if } a_i \in S_1'. \tag{14}$$

For $a_i, a_j \in S_1'$ with $i \ne j$, the equation $x_i = x_j$ implies that

$$\chi \le k^3 (\log\log k)^{1-\varepsilon/2}, \tag{15}$$

by (10), (14) and $\gcd(m,d)=1$. Consequently, we conclude from (12) and (15) that

$$x_i \neq x_j \quad \text{if } a_i, a_j \in S_1' \text{ and } i \neq j. \tag{16}$$

We denote by $b_1,\ldots,b_s$ all integers between $k(\log k)^{-2c}$ and $k(\log\log k)^{1-\varepsilon/2}$ such that every proper divisor of b_i is less than or equal to $k(\log k)^{-2c}$. Now, we apply Brun's Sieve to derive that

$$s \le k(\log\log k)^{-\varepsilon/2}.$$

We write S_2' for the set of all $a_i \in S_1'$ with $a_i \ge k(\log k)^{-2c}$. Then $|S_2'| \ge \varepsilon k/4$. Further, we observe that every element of S_2' is divisible by at least one b_i. Let S_3' be the maximal subset of S_2' such that every b_i appears in the factorisation of at most two elements of S_3'. Then

$$|S_3'| \le 2s \le 2k(\log\log k)^{-\varepsilon/2}.$$

We write S_4' for the complement of S_3' in S_2'. If $a_i = a_{i_1} \in S_4'$, there exist $a_{i_2}, a_{i_3} \in S_3'$ and b_ν such that a_{i_1}, a_{i_2} and a_{i_3} are divisible by b_ν. Also, we observe that $|S_4'| \ge \varepsilon k/8$. We put

$$B_1 = b_\nu^{-1} a_{i_1}, \qquad B_2 = b_\nu^{-1} a_{i_2}, \qquad B_3 = b_\nu^{-1} a_{i_3}$$

and

$$R = b_\nu^{-1}\left(d_{i_2} - d_{i_1}\right), \qquad R^{-1} = b_\nu^{-1}\left(d_{i_3} - d_{i_1}\right).$$

Since $\gcd(m,d)=1$, we observe that B_1, B_2, B_3, R and R' are integers of absolute values not exceeding $(\log k)^{3c}$. By (10), we have

$$B_2 B_3 (d^{-1} x_{i_2} x_{i_3})^2 = \left(B_1\left(\frac{x_i}{\sqrt{d}}\right)^2 + R\right)\left(B_2\left(\frac{x_i}{\sqrt{d}}\right)^2 + R'\right).$$

There are at most $32(\log k)^{15c}$ of these equations. Now, we apply Theorem 1 of Evertse and Silverman [5], $|S_4'| \ge \varepsilon k/8$ and (16) to conclude that

$$\log k \le (\log k)^{cc'} \tag{17}$$

where c' is an effectively computable number depending only on ε and $\omega(d)$. Let $c = (2c')^{-1}$ to notice that (17) is not possible.

(b) We do not give the details, since they are similar to the proof of Corollary 1 of [12]. See Remark (ii) of [12], p. 343.

3. Let $\varepsilon > 0$. We suppose that k exceeds a sufficiently large effectively computable number depending only on ε. Let $F(k)$ be a non-decreasing function of k such that $F(k) > k$. We write

$$T(d) = \{m, m+d, \ldots, m+(k-1)d\}.$$

Let $T'(d)$ be the subset of $T(d)$ of all elements $m+id$ satisfying $P(m+id) \le k$. For every prime q with $k < q < F(k)$, we let $i_q \in [0,q)$ be such that

$m + i_q d \equiv 0 \pmod q$ (if such an i_q exists). We denote by $T(d, F(k))$ the subset of $T(d)$ obtained by deleting $m + i_q d$ for all primes q satisfying $k < q < F(k)$. We put

$$|T(d, F(k))| = t(d, k) = t$$

and we write

$$T(d, F(k)) = \{m + d_1 d, \ldots, m + d_t d\} \tag{18}$$

where $d_1, \ldots, d_t$ are distinct integers in the interval $[0, k)$. We observe that

$$t \geq k - \pi(F(k)). \tag{19}$$

The following lemma is useful for the proof of Theorem 1 and Corollary 1.

Lemma 1. *Let $\varepsilon > 0$ and $\chi > k^l$. There exists an effectively computable number C_{12} depending only on ε such that for $k \geq C_{12}$, we have*

$$|T'(d)| \leq (l^{-1} + \varepsilon)k. \tag{20}$$

Proof. Let $\varepsilon_1 = \varepsilon/2$. For $\varepsilon_1 k \leq i < k$, we observe that

$$m + id \geq i\chi/(k-1) \geq \varepsilon_1 \chi \geq \varepsilon_1 k^l.$$

Now, we apply Lemma 2 of [11] with T the set of all $m+id$ such that $i \geq \varepsilon_1 k$ and $P(m + id) \leq k$. Then

$$|T'(d)| \leq \frac{k \log k}{\log(\varepsilon_1 k^l)} + \varepsilon_1 k + \pi(k) \leq (l^{-1} + \varepsilon)k. \ \blacksquare$$

Proof of Theorem 1. Put $d = 1$. We may assume that $k \geq c_1$ where c_1 is a sufficiently large effectively computable number depending only on ε. We shall apply the results of Shorey on equation (1) with $d = 1$ stated in the beginning of Section 1 without reference in the proof of Theorem 1.

Suppose $l = 2$. Put $F(k) = (1-\varepsilon)k \log\log k$. By (19) and Prime Number Theorem, we observe that

$$t > k - \left(1 - \frac{\varepsilon}{2}\right)k\frac{\log\log k}{\log k} \geq 2. \tag{21}$$

By (21),(20) and (18), we derive that there exists an i with $1 \leq i \leq t$ such that $m + d_i$ is divisible by a prime $> k$. Furthermore, we may suppose that equation (1) with $d = 1, l = 2$ and $k \geq c_1$ is satisfied. Therefore, inequality (3) with ε replaced by $\varepsilon/2$ is valid. This contradicts (21).

Next suppose $l > 2$. Put $F(k) = (1 - \nu_l - \varepsilon)k \log k$. Then, we derive from (19), (5) and (20) that

$$t > \left(\nu_l + \frac{\varepsilon}{2}\right)k > (l^{-1} + \varepsilon)k \geq |T'(1)|. \tag{22}$$

Consequently, we may suppose that (1) with $d = 1$, $l > 2$ and $k \geq c_1$ is satisfied. Hence, we conclude (5), which contradicts (22).

Now suppose that $l \geq c_1$. Put $F(k) = (1-\varepsilon)k \log k$. Then

$$|T'(1)| \leq \left(l^{-1} + \frac{\varepsilon}{4}\right)k < \frac{\varepsilon k}{2} \leq t \tag{23}$$

whenever c_1 is sufficiently large. Therefore, we may assume that (1) with $d = 1, k \geq c_1$ and $l \geq c_1$ is satisfied. Hence, we conclude (6), which contradicts (23) if c_1 is sufficiently large.

Proof of Corollary 1. (a) We may assume that k exceeds a sufficiently large effectively computable number c_2 depending only on ε and $\omega(d)$. Put $F(k) = (1-\varepsilon)k \log\log\log k$. Then

$$t > k - \left(1 - \frac{\varepsilon}{2}\right)k \frac{\log\log\log k}{\log k}$$

and we may suppose that equation (1) with $l = 2$, $k \geq c_2$ is satisfied. On the other hand, we apply Theorem 2(a) to conclude (7) with ε replaced by $\varepsilon/2$. This is a contradiction.

(b) We may assume that $C_{11} \leq C_9$ so that (9) implies (8). Now, we take $F(k) = (1-\varepsilon)kh(k)$ to argue as above for deriving Corollary 1(b) from Theorem 2(b).

References

[1] P. Erdős, *Note on the product of consecutive integers (I)*, J. London Math. Soc. 14 (1939), 194–198.

[2] —, *On the product of consecutive integers III*, Indag. Math. 17 (1955), 85–90.

[3] P. Erdős and J. Turk, *Products of integers in short intervals*, Acta Arith. 44 (1984), 147–174.

[4] J.-H. Evertse, *On the equation $ax^n - by^n = c$*, Compositio Math. 47 (1982), 289–315.

[5] J.-H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to $Y^n = f(X)$*, Math. Proc. Cambridge Philos. Soc. 100 (1986), 237–248.

[6] T. N. Shorey, *On gaps between numbers with a large prime factor II*, Acta Arith. 25 (1974), 365–373.

[7] —, *Perfect powers in values of certain polynomials at integer points*, Math. Proc. Cambridge Philos. Soc. 99 (1986), 195–207.

[8] —, *Perfect powers in products of integers from a block of consecutive integers*, Acta Arith. 49 (1987), 71–79.

[9] —, *Some exponential diophantine equations*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge University Press, 1988, 217–229.

[10] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge University Press, 1986.

[11] —, —, *On the greatest prime factor of an arithmetical progression II*, Acta Arith. 53 (1990), 499–504.

[12] —, —, *Perfect powers in products of terms in an arithmetical progression*, Compositio Math. 75 (1990), 307–344.

[13] T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression III*, in: Diophantine Approximation and Transcendental Numbers, Luminy 1990, Ph. Philippon (ed.), to appear.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY 400005, INDIA

MATHEMATICAL INSTITUTE
R. U. LEIDEN
P.O. BOX 9512
2300 RA LEIDEN, THE NETHERLANDS

Received on 8.10.1991 (2179)