COMPOSITIO MATHEMATICA

T. N. SHOREY
R. TIJDEMAN

Perfect powers in arithmetical progression (II)

Compositio Mathematica, tome 82, n° 1 (1992), p. 107-117
<http://www.numdam.org/item?id=CM_1992__82_1_107_0>

Compositio Mathematica **82**: 107–117, 1992.

Perfect powers in arithmetical progression (II)

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

[1]*School of Mathematics, Tata 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 November 1989; accepted 22 August 1991

Section 1

It is an old question how long arithmetical progressions of equal powers of positive integers can be. There exist infinitely many triples of coprime squares in arithmetical progression, but Fermat proved that there are no four squares in arithmetical progression, see [8, p. 21]. Dénes [2] conjectured that for $l \geqslant 3$ there are no three l-th powers in arithmetical progression, and proved this assertion for $3 \leqslant l \leqslant 30$ and for sixty other prime values of l. Faltings' celebrated result [5] implies that for any $l \geqslant 5$ there are only finitely many triples of coprime l-th perfect powers in arithmetical progression. Without loss of generality we can restrict our attention to the following situation:

$$\left.\begin{array}{l} l \text{ is a prime number, } l \geqslant 3, \text{ and } m, d \text{ and } k \text{ are positive} \\ \text{integers satisfying } \gcd(m, d) = 1 \text{ and } k \geqslant 3 \text{ such that each} \\ \text{of the numbers } m, m + d, \ldots, m + (k-1)d \text{ is an } l\text{-th perfect power.} \end{array}\right\} \quad (1)$$

Let d_1 be the maximal divisor of d such that all the prime factors of d_1 are $\equiv 1 (\mathrm{mod}\, l)$. Similarly, we define m_1 as the maximal divisor of m such that all the prime factors of m_1 are $\equiv 1 (\mathrm{mod}\, l)$. For an integer v with $|v| > 1$, we write $p(v)$, $P(v)$, $Q(v)$ and $\omega(v)$, respectively, for the least prime factor of v, the greatest prime factor of v, the greatest square free factor of v and the number of distinct prime divisors of v. Further, we set $p(\pm 1) = P(\pm 1) = Q(\pm 1) = 1$ and $\omega(\pm 1) = 0$. We write $p(l, 1)$ for the least prime $\equiv 1 (\mathrm{mod}\, l)$. Recently Heath-Brown announced that he has proved

$$p(l, 1) < l^{10} \qquad \text{if } l \geqslant C \quad (2)$$

for some effectively computable absolute constant C. Until now the best exponent was 16, see Wei [12].

It follows from the above mentioned results of Dénes and Faltings that if (1)

holds then k is bounded by some number depending only on l. We showed in [10] that there exists an upper bound for k depending only on $\omega(d)$. In fact, we proved in [10] that (1) implies that

$$\prod_{p<k/2} p \quad \text{divides } d \tag{3}$$

and that

$$\log d \geqslant 2k^2/13 \quad \text{if } k \geqslant C_1. \tag{4}$$

Furthermore, it follows from formula (2.7) of [11] that

$$d_1 > 1 \quad \text{if } k \geqslant C_1. \tag{5}$$

Here C_1 is an effectively computable absolute constant. In this paper, we find an upper bound for k depending only on $\omega(d_1)$. More precisely, we prove

THEOREM 1. *Let $\varepsilon > 0$. There exists an effectively computable number C_2 depending only on ε such that* (1) *with $k \geqslant C_2$ implies that*

$$2^{\omega(d_1)} > (1-\varepsilon)k. \tag{6}$$

Theorem 1 sharpens the assertion of Corollary 1 of [11] under a stronger assumption. We derive the following result from Theorem 1, the Brun-Titchmarsh Theorem and (3).

COROLLARY 1. *Let $\varepsilon > 0$ and $\eta(\varepsilon) = (1-\varepsilon)/\log 2$. There exists an effectively computable number C_3 depending only on ε such that* (1) *with $k \geqslant C_3$ implies that*

$$2P(d_1) \geqslant \eta(\varepsilon) l \log k \log\log k \tag{7}$$

and

$$\log Q(d_1) \geqslant \eta(\varepsilon)(\log k)^2. \tag{8}$$

Observe that (3) gives stronger results than (7) for small values of l. For example, we see from (3) and the Prime Number Theorem for arithmetical progressions that (1) implies that

$$P(d_1) > k/4$$

if l does not exceed a fixed power of $\log k$ and k is sufficiently large.

It is clear from (3) that it is not possible to obtain an inequality analogous to (7) for $p(d_1)$. In fact, $p(d_1)$ is bounded whenever l is bounded. More generally, we see from (3) and (2) that if (1) holds with k exceeding a sufficiently large absolute constant, then

$$p(d_1) \leqslant l^{10} \quad \text{if } l < C_4 k^{1/10}$$

where $C_4 = 2^{-1/10}$.

Next we consider analogous results for m.

THEOREM 2. (a) *There exists an effectively computable absolute constant* $C_5 > 0$ *such that* (1) *implies that*

$$\log(m+1) \geqslant C_5 k^2. \tag{9}$$

(b) *There exist effectively computable absolute constants* C_6 *and* $C_7 > 0$ *such that* (1) *with* $k \geqslant C_6$ *implies that*

$$l^{\omega(m_1)} \geqslant C_7 k, \tag{10}$$

$$p(m_1) > kl \tag{11}$$

and

$$Q(m_1) \geqslant C_7 k^{1+\omega(m_1)}. \tag{12}$$

COROLLARY 2. *If* (1) *holds then*

$$m_1 > 1 \quad \text{for } k \geqslant C_6.$$

Finally, we prove a result involving both m and d,

THEOREM 3. *There exists an effectively computable absolute constant* C_8 *such that* (1) *with* $k \geqslant C_8$ *implies that*

$$P(m-d) \geqslant k.$$

Section 2. Proof of Theorem 1

We may assume that (1) with $k \geqslant c$ is valid where c is a sufficiently large effectively computable number depending only on ε. Further, by the result of

Dénes mentioned in Section 1, we may suppose that $l > 30$. The case $l \leqslant 4\omega(d_1) + 2$ is treated in the following lemma.

LEMMA 1. *Suppose* (1) *is satisfied with* $30 < l \leqslant 4\omega(d_1) + 2$. *Then*

$$\omega(d_1) > \tfrac{3}{2}\log k. \tag{13}$$

Proof. First we consider the case that $3l \leqslant \omega(d_1)$. Then there exists a positive integer n satisfying

$$\frac{5\omega(d_1)}{l} < n \leqslant \frac{16\omega(d_1)}{3l}.$$

Consequently, there exists a divisor d' of d_1 such that

$$\omega(d') = n \leqslant \frac{16\omega(d_1)}{3l} \tag{14}$$

and

$$d' \geqslant d_1^{n/\omega(d_1)} > d_1^{5/l}.$$

Therefore, by (2.1) of [11],

$$d' \geqslant C_5 d^{5(l-2)/l^2} \tag{15}$$

where C_5 is the absolute constant appearing in (2.1) of [11]. Further, since $l > 30$, we observe that

$$\frac{5(l-2)}{l^2} \geqslant \frac{9}{2l}. \tag{16}$$

Now we proceed to apply Theorem 1(b) of [11]. For this, we observe from (15), (16) and (4) (or (2.13) of [11]) that

$$d' \geqslant C_8 l^{-1} d^{4/l}$$

where C_8 is the constant appearing in (2.4) of [11]. Hence, by theorem 1(b) of [11],

$$l^{\omega(d')} > \frac{k}{\log k}$$

which, together with (14), implies that

$$\omega(d_1) \geqslant \frac{3l}{16}\frac{\log(k/\log k)}{\log l} > \frac{l\log k}{6\log l} > \frac{3}{2}\log k, \tag{17}$$

since $l > 30$.

Thus we may assume that $3l > \omega(d_1)$. Then we may suppose that $l > 200$, otherwise we apply Corollary 3 of [11] to conclude that $k < c$.

Next we consider the general case $30 < l \leqslant 4\omega(d_1) + 2$. Then there exists a positive integer n with

$$\frac{5\omega(d_1)}{l} < n \leqslant \frac{10\omega(d_1)}{l}$$

and a divisor d' of d_1 satisfying

$$\omega(d') \leqslant \frac{10\omega(d_1)}{l}, \quad d' \geqslant d_1^{5/l} \geqslant d^{9/2l}.$$

Now, we apply Theorem 1(b) of [11] as above, to conclude that

$$\omega(d_1) > \frac{l\log k}{12\log l} \tag{18}$$

which, since $l > 200$, implies that $\omega(d_1) > \frac{3}{2}\log k$. □

To complete the proof of Theorem 1, we consider the case $l > 4\omega(d_1) + 2$. Then, by (5), there exists a divisor d' of d_1 such that

$$\omega(d') = 1 \quad \text{and} \quad d' \geqslant d_1^{1/\omega(d_1)}.$$

Further, by (2.1) of [11], we observe that

$$d' \geqslant C_5 d^{4(1+1/(l-3))/l} \tag{19}$$

where C_5 is the absolute constant appearing in (2.1) of [11]. Now we proceed to apply Lemma 8 of [11] with $f(x) = \log x$. First we observe from (19) and (2.7) of [11] that

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

Also it is easy to see that $|S_1| \leqslant \pi(k)$ where S_1 is the set appearing in Lemma 8 of

[11]. For this, observe that, by (1), for every prime $p \leqslant k$ there is at most one μ with $0 \leqslant \mu < k$ such that $m + \mu d$ is divisible by p. (In fact, (3) is an immediate consequence of this assertion.) Hence we apply Lemma 8 of [11] to conclude that

$$l \geqslant (1 - \varepsilon_1)k, \qquad \varepsilon_1 = \varepsilon/2. \tag{20}$$

We write

$$m + \mu d = x_\mu^l \quad \text{for } 0 \leqslant \mu < k. \tag{21}$$

Therefore, for $\mu > \nu \geqslant 0$, we have

$$(\mu - \nu)d = (x_\mu - x_\nu)\left(\frac{x_\mu^l - x_\nu^l}{x_\mu - x_\nu}\right). \tag{22}$$

We put

$$x_{\mu,\nu} = \frac{x_\mu^l - x_\nu^l}{x_\mu - x_\nu} \quad \text{for } \mu > \nu \geqslant 0.$$

Except possibly l, every prime factor of $x_{\mu,\nu}$ is $\equiv 1 \pmod{l}$ and $l^2 \nmid x_{\mu,\nu}$. In particular, we observe from (20) that

$$p(x_{\mu,\nu}) \geqslant l \geqslant (1 - \varepsilon_1)k$$

which implies that

$$\gcd(x_{\mu,\nu}, \mu - \nu) = 1 \quad \text{for } \mu > \nu \geqslant [2\varepsilon_1 k] - 2. \tag{23}$$

Now we fix $\nu = [2\varepsilon_1 k] - 2$. We conclude from (22) that for $\mu > \nu$ there exist positive integers $d_{1,\mu} = d_{1,\mu,\nu}$ and $d_{2,\mu} = d_{2,\mu,\nu}$ such that

$$d = d_{1,\mu} d_{2,\mu}, \quad \gcd(d_{1,\mu}, d_{2,\mu}) = 1 \text{ or } l$$

and

$$d_{1,\mu} \mid x_{\mu,\nu}, \qquad d_{2,\mu} \mid x_\mu - x_\nu.$$

Furthermore, we derive from (23) that $x_{\mu,\nu} = d_{1,\mu}$ and $d_{1,\mu} l^{-\delta}$ is a divisor of d_1

where

$$\delta = \begin{cases} 1 & \text{if } l \mid d, \\ 0 & \text{if } l \nmid d. \end{cases}$$

For $\mu_1 > \mu_2 > \nu$, we observe that $x_{\mu_1,\nu} > x_{\mu_2,\nu}$. Now we apply the Box Principle to conclude that

$$2^{\omega(d_1)} \geqslant k - \nu - 1 > (1 - \varepsilon)k. \qquad \square$$

PROOF OF COROLLARY 1. Let $\varepsilon > 0$ and $\varepsilon_1 = \varepsilon/2$. Suppose that (1) with $k \geqslant C_3$ is valid. Further, we may assume that C_3 is sufficiently large. Now we see from (6) that

$$\omega(d_1) \geqslant (1 - \varepsilon_1) \frac{\log k}{\log 2}. \tag{24}$$

We recall that every prime divisor of d_1 is $\equiv 1 (\mathrm{mod}\, l)$ and we apply the Brun-Titchmarsh Theorem to derive (7) from (24).

Next we proceed to prove (8). First we assume that $l \geqslant 4\omega(d_1) + 2$. Now we apply Lemma 8 of [11] as in the proof of Theorem 1 to conclude (20). Further we observe that

$$\log Q(d_1) \geqslant \omega(d_1) \log l. \tag{25}$$

We combine (25), (24) and (20) to derive (8) if $l > 4\omega(d_1) + 2$.

Thus we may assume $l \leqslant 4\omega(d_1) + 2$. Then we apply Theorem 1(b) of [11] as in the proof of Lemma 1 to conclude (18). We combine (25) and (18) to derive

$$\log Q(d_1) \geqslant (l \log k)/12.$$

Thus we may suppose that $l \leqslant 12\eta(\varepsilon) \log k$. Then we see from (3) and the Prime Number Theorem for arithmetical progressions that

$$\log Q(d_1) \geqslant k/(\log k)^3$$

which implies (8). $\square$

Section 3

We denote by $c_1, \ldots, c_9$ effectively computable absolute constants. Suppose that (1) is valid with $k \geqslant c_1$ where c_1 is sufficiently large. We write (21). As already remarked, for every prime $q \leqslant k$ there is at most one μ with $0 \leqslant \mu < k$ such that $m + \mu d$ is divisible by q. Therefore there exists a set T with $|T| \geqslant k - \pi(k)$ consisting of integers μ satisfying $0 \leqslant \mu < k$ and $p(x_\mu) > k$. Further, for $\mu \in T$ and $\nu \in T$ with $\mu > \nu$, we observe from (21) that

$$\mu x_\nu^l - \nu x_\mu^l = (\mu - \nu)m.$$

Then we have

$$\frac{\mu}{\gcd(\mu, \nu)} x_\nu^l - \frac{\nu}{\gcd(\mu, \nu)} x_\mu^l = \frac{\mu - \nu}{\gcd(\mu, \nu)} m.$$

We apply the sieve-theoretic Lemma 1 of Erdös [3] to conclude that there exist positive integers P, Q and R such that

$$\max(P, Q, R) \leqslant c_2, \quad \gcd(P, Q) = 1$$

and that

$$Px_\nu^l - Qx_\mu^l = Rm \tag{26}$$

is satisfied by at least $c_3 k$ pairs x_μ, x_ν with $p(x_\mu) > k$, $p(x_\nu) > k$ and $\gcd(x_\mu, x_\nu) = 1$.

PROOF OF THEOREM 2(a). We may assume that $k \geqslant c_1$, otherwise (9) follows immediately. Now we apply a theorem of Baker [1] on linear forms in logarithms to conclude from (26) that

$$m \geqslant x_\mu^{l - c_4 \log l}$$

which implies that

$$m \geqslant d^{1 - (c_5 \log l)/l}. \tag{27}$$

This inequality is trivial if $c_5 \log l \geqslant l$ which implies that $l \leqslant c_6$. If $l \leqslant c_6$, we apply an estimate of Feldman [6] on the magnitude of integral solutions of Thue's equation (cf. [9], Chapter 5) to (26) for deriving

$$m \geqslant d^{c_7} \quad \text{if } l \leqslant c_6. \tag{28}$$

Now we combine (27) and (28) to obtain $m \geqslant d^{c_8}$ which, together with (4), implies (9).

PROOF OF THEOREM 2(b). Assume (1). We may suppose that $k \geqslant c_1$ and, by part (a), that $m \geqslant c_2^5$. Then there are at least $c_3 k$ pairs x_μ, x_ν with $p(x_\mu) > k$, $p(x_\nu) > k$ and $\gcd(x_\mu, x_\nu) = 1$ satisfying (26). Observe that

$$\gcd(P, m) = \gcd(Q, m) = \gcd(x_\mu, x_\nu) = 1.$$

Now we apply Theorem 2 of Evertse [4] on an upper bound for the number of solutions of (26) to conclude that

$$c_3 k \leqslant R(l, m) + 2 \leqslant c_9 l^{\omega(m_1)}$$

which implies (10).

We put $p = p(m_1)$. Then, by Corollary 2, we observe that $p \geqslant 2$. Since $\mathrm{ord}_p(m) \geqslant l$ and $\gcd(m, d) = 1$, we see that $\mathrm{ord}_p(m + pd) = 1$. If $p < k$, then this is not possible. Thus we derive that

$$p \geqslant k. \tag{29}$$

By (21), we have

$$\mu d \equiv x_\mu^l (\mathrm{mod}\, p) \quad \text{for } 0 \leqslant \mu < k. \tag{30}$$

Further, by (29) and $\gcd(m, d) = 1$, we observe that

$$\mu d \not\equiv \nu d (\mathrm{mod}\, p) \quad \text{for } 0 \leqslant \nu < \mu < k. \tag{31}$$

On the other hand, since $p \equiv 1 (\mathrm{mod}\, l)$, we see that $x_0^l, x_1^l, \ldots, x_{k-1}^l$ lie in at most $(p-1)/l$ distinct residue classes mod p. Hence we conclude from (30) and (31) that $(p-1)/l \geqslant k$ which implies (11). Finally we observe that $Q(m_1) \geqslant p^{\omega(m_1)}$ which, together with (11) and (10), implies (12). □

Section 4. Proof of Theorem 3.

We denote by c_{10}, c_{11} and c_{12} effectively computable positive absolute constants. Assume (1) with $k \geqslant c_{10}$ where c_{10} is sufficiently large. Put $|m - d| = M$. Observe that $M \neq 0$, since $\gcd(m, d) = 1$. By (21), we have

$$M = |2x_0^l - x_1^l|.$$

As in the proof of Theorem 2(a), we derive from the theorems of Baker and Feldman that

$$\log M \geqslant c_{11} \log d$$

which, together with (4), implies

$$\log M \geqslant c_{12} k^2. \tag{32}$$

For a prime $q \leqslant k$ dividing $m - d$, we see from (21) that $\operatorname{ord}_q(m - d + qd) \geqslant l$. Therefore, since $\gcd(m, d) = 1$, we derive that $\operatorname{ord}_q(m - d) \leqslant 1$ for every prime $q \leqslant k$. Assume that $P(M) \leqslant k$. Then

$$\log M \leqslant \sum_{q \leqslant k} \log q \leqslant 2k$$

which contradicts (32). □

REMARK. Estimate (9) can be sharpened. Suppose that (1) is satisfied and let $\varepsilon > 0$. We refer to (27) and (4) to derive that

$$\log(m + 1) \geqslant \left(\frac{2}{13} - \varepsilon\right) k^2 \quad \text{if } \min(k, l) \geqslant C_9$$

where C_9 is an effectively computable number depending only on ε. For all l, we apply Theorem 1 of [7] to (26), together with (4) and $l > 30$, to obtain

$$\log(m + 1) \geqslant \left(\frac{29}{403} - \varepsilon\right) k^2 \quad \text{if } k \geqslant C_{10}$$

where C_{10} is an effectively computable number depending only on ε.

References

1. A. Baker, A sharpening of the bounds for linear forms in logarithms I, *Acta Arith.* 21, 117–129 (1972).
2. P. Dénes, Über die Diophantische Gleichung $x^l + y^l = cz^l$, *Acta Math.* 88, 241–251 (1952).
3. P. Erdös, Note on the product of consecutive integers (II), *J. London Math. Soc.* 14, 245–249 (1939).
4. J.-H. Evertse, On the equation $ax^n - by^n = c$, *Compositio Math.* 47, 289–315 (1982).
5. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* 71, 349–366 (1983).

6. N. I. Feldman, An effective sharpening of the exponent in Liouville's theorem (Russian), *Izv. Akad. Nauk SSSR Ser. mat.* 35, 973–990 (1971), English trans.: *Math. USSR Izv.* 5, 985–1002.
7. J. Mueller, Counting solutions of $|ax^r - by^r| \leqslant h$, *Quart. J. Math. Oxford* (2), 38, 503–513 (1987).
8. L. J. Mordell, *Diophantine Equations*, Academic Press, London (1969).
9. T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics 87 (1986).
10. T. N. Shorey and R. Tijdeman, Perfect powers in arithmetical progression, *J. Madras Univ.*, Section B, 51, 173–180 (1988).
11. T. N. Shorey and R. Tijdeman, Perfect powers in products of terms in an arithmetical progression, *Comp. Math.* 75, 307–344 (1990).
12. W. Wei, On the least prime in an arithmetic progression, *Acta Math.* Sinica 29, 826–836 (1986)