T. N. SHOREY
R. TIJDEMAN

Perfect powers in products of terms in an arithmetical progression (II)

Compositio Mathematica, tome 82, n° 2 (1992), p. 119-136

<http://www.numdam.org/item?id=CM_1992__82_2_119_0>
Perfect powers in products of terms in an 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 11 December 1989; accepted 22 August 1991

Section 1

For an integer $x$ with $|x| > 1$, we write $p(x)$, $P(x)$, $Q(x)$ and $\omega(x)$, respectively, for the least prime factor of $x$, the greatest prime factor of $x$, the greatest square free factor of $x$ and the number of distinct prime factors of $x$. Further, we put $p(\pm 1) = P(\pm 1) = Q(\pm 1) = 1$ and $\omega(\pm 1) = 0$. We consider the equation

$$m(m + d) \cdots (m + (k - 1)d) = by^l$$

(1)

in positive integers $b, d, k, l, m, y$ subject to $P(b) \leq k$, $\gcd(m, d) = 1$, $k > 2$, $l > 1$ and $P(y) > k$. There is no loss of generality in assuming that $l$ is a prime number. Let $d_1$ be the maximal divisor of $d$ such that all the prime factors of $d_1$ are $\equiv 1 \pmod{l}$. Similarly, we define $m_1$ as the maximal divisor of $m$ such that all the prime divisors of $m_1$ are $\equiv 1 \pmod{l}$. For $\varepsilon > 0$, we put $\eta(\varepsilon) = (1 - \varepsilon)/\log 2$,

$$\eta'(l, \varepsilon) = \eta(l, \varepsilon) = \begin{cases} (1 - \varepsilon)/\log 2 & \text{if } l > 30 \\ (1 - \varepsilon)/\log l & \text{if } l \leq 30 \end{cases}$$

and

$$\tau(l, \varepsilon) = \tau(l, \varepsilon) = \begin{cases} 2 & \text{if } l > 30 \\ l + \varepsilon & \text{if } l \leq 30. \end{cases}$$

Notice that

$$\eta'(l, \varepsilon) \geq (1 - \varepsilon)/\log 30 \text{ and } \tau(l, \varepsilon) \leq 30 + \varepsilon$$

for every $l$. We shall follow the above notation without reference.
Erdős and Selfridge [4] confirmed an old conjecture by proving that the product of two or more consecutive positive integers is never a power. Marszalek [6] showed that (1) with \( b = 1 \) implies that \( k \) is bounded by an effectively computable number \( C \) depending only on \( d \). Shorey [7] showed that we can take \( C \) depending only on \( P(d) \) whenever \( l \geq 3 \). According to Shorey and Tijdeman [9], Corollary 3, the number \( C \) can be taken to depend only on \( l, \omega(d_1) \) if \( l \geq 7 \) and only on \( \omega(d) \) if \( l \leq 5 \). Further, Shorey and Tijdeman [9], Corollary 4(a), proved that (1) implies that

\[
\log d_1 \geq C_1 \frac{\log k \log \log k}{\log \log \log k}, \quad \log d_1 \geq C'_1 \log k \log \log k
\]  

(2)

where \( C_1 > 0 \) is an effectively computable absolute constant and \( C'_1 > 0 \) is an effectively computable number depending only on \( l \). In this paper, we sharpen (2) as follows:

**THEOREM 1.** Let \( \varepsilon > 0 \). There exists an effectively computable number \( C_2 \) depending only on \( \varepsilon \) such that (1) with \( k \geq C_2 \) and \( l \geq 7 \) implies that

\[
\log d_1 \geq \eta'(\varepsilon) \log k \log \log k.
\]  

(3)

Next, we extend the result of Shorey mentioned above by proving that (1) implies that \( k \) is bounded by an effectively computable number depending only on \( p(d_1)/l \) and \( \omega(d_1) \). More precisely, we prove

**THEOREM 2.** Let \( \varepsilon > 0 \). There exist effectively computable numbers \( C_3 \) and \( C_4 > 0 \) depending only on \( \varepsilon \) such that (1) with \( k \geq C_3 \) implies that

\[
p(d_1) \geq C_4 k l (\tau(\varepsilon))^{-\omega(d_1)} \quad \text{if } l \geq 7
\]  

(4)

and

\[
p(d_1) \geq C_4 k l (\tau(\varepsilon))^{-\omega(d)} \quad \text{if } l \in \{2, 3, 5\}.
\]  

(5)

We apply Theorem 2 to obtain the following quantitative version of the result of Shorey.

**COROLLARY 1.** Let \( \varepsilon > 0 \). There exists an effectively computable number \( C_5 \) depending only on \( \varepsilon \) such that (1) with \( k \geq C_5 \) implies that

\[
2P(d_1) \geq \eta'(\varepsilon) l \log k \log \log k \quad \text{if } l \geq 7,
\]  

(6)

\[
P(d) \geq \eta'(\varepsilon) l \log k \log \log k \quad \text{if } l \in \{2, 3, 5\}
\]  

(7)
and

\[ Q(d_1) \geq \max(lk^{1-\varepsilon}, k^{2-\varepsilon}) \quad \text{if } l \geq 7, \quad (8) \]

\[ Q(d) \geq \max(lk^{1-\varepsilon}, k^{2-\varepsilon}) \quad \text{if } l \in \{2, 3, 5\}. \quad (9) \]

If \( m, m + d, \ldots, m + (k - 1)d \) are \( l \)th perfect powers, we may, by a result of Dénes [2], assume that \( l > 30 \) and therefore, (6) includes (6) of [10]. Further, under this restrictive assumption, it is shown in [10] that (8) can be replaced by

\[ \log Q(d_1) \geq \eta(\varepsilon)(\log k)^2 \quad \text{if } k \geq C_5. \]

Further, we observe from Theorem 2 that for \( k \geq C_3 \) and \( l \geq 7 \), either

\[ (\pi(\varepsilon))^{\omega(d_1)} \geq k^{1-\varepsilon} \quad (10) \]

or

\[ p(d_1) \geq c_d l k^\varepsilon. \quad (11) \]

As observed in [10], the assertion that (1) implies (11) is false. Also, notice that (1) with \( l \leq 4\omega(d_1) + 2 \) implies (10). See Lemma 6. In the opposite case we prove

**THEOREM 3.** Suppose that (1) with \( l > 4\omega(d_1) + 2 \) is satisfied. Then

(a) There exists an effectively computable absolute constant \( C_6 > 0 \) such that

\[ p(d_1) \geq C_6 k. \quad (12) \]

(b) There exists an effectively computable absolute constant \( C_7 > 0 \) such that

\[ p(d_1) \geq C_7 l \log k \quad (13) \]

or

\[ p(m_1) \geq lk/(33C_7 \log k). \quad (14) \]

In particular, we derive from Theorem 3 that (1) with \( l > 4\omega(d_1) + 2 \) implies that \( k \) is bounded by an effectively computable number depending only on \( p(d_1)/l \) and \( p(m_1)/l \). Next, we give lower bounds for \( P(m) \). Shorey [8] showed that there exist effectively computable absolute constants \( C_8 \) and \( C_9 \) such that (1) with \( k \geq C_8 \) implies that

\[ m \geq d^{1-C_9\Delta_1} \quad \text{where } \Delta_1 = l^{-1}(\log l)^2(\log l + 1). \quad (15) \]
In particular, we derive from (15) that (1) implies that

$$m \geq d^{1/2} \quad \text{if } \min(k, l) \geq C_{10}$$

(16)

where $C_{10}$ is an effectively computable absolute constant. We combine this result with (2) and Corollary 3 of [9] to derive that (1) implies that $k$ is bounded by an effectively computable number $C_{11}$ depending only on $m$ and $\omega(d)$. We extend this result by showing that we can take $C_{11}$ depending only on $P(m)$ and $\omega(d)$. This is a consequence of the following result (Theorem 4(a)) and Corollary 3 of [9]. Compare Theorem 4(b) with Theorem 3 of [10].

**THEOREM 4(a).** Let $\varepsilon > 0$. There exists an effectively computable number $C_{12}$ depending only on $\varepsilon$ such that (1) with $k \geq C_{12}$ and $l > 4\omega(d) + 2$ implies that

$$\min_{0 \leq \mu < k} P(m + \mu d) \geq k^{1/3 - \varepsilon}. \quad (17)$$

(b) There exists an effectively computable absolute constant $C_{13}$ such that (1) with $k \geq C_{13}$, $l > 4\omega(d) + 2$ and $b = 1$ implies that

$$P(m - d) > k. \quad (18)$$

**Section 2**

For $0 \leq i < k$, we see from (1) that

$$m + id = A_iX_i^l \quad (19)$$

where

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

Notice that

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

We put

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

For $\alpha > 0$, we denote by $S_2(\alpha)$ the set of all $A_\mu \in S_1$ satisfying $A_\mu \leq \alpha k$. Further,
Let $T$ be the set of all $y$ with $0 \leq \mu < k$ and $A_\mu \in S_2$. We shall always write

$$p = p(d_1), \quad q = p(m_1). \quad (20)$$

We assume that $k$ exceeds some effectively computable large absolute constant. Then, by (2), we have $p \geq 2$. Finally, as stated in Section 1, we assume in (1) that $P(y) > k$. Therefore, by (1),

$$m + (k - 1)d \geq k^l$$

which implies that

$$m + d \geq k^{l-1}. \quad (21)$$

In addition to the notation of Section 1, we shall follow the above notation without reference.

In this section, we prove lemmas for the proofs of our theorems. We start with an estimate on the number of elements of a subset of $S_1$.

**Lemma 1.** Let $S_3$ be a subset of $S_1$ and $z_3$ be the maximum of the elements of $S_3$. Then

$$|S_3| \leq (z_3 + p - 1)/l \quad (22)$$

where $p$ is given by (20).

**Proof.** First, since $p \equiv 1 \pmod{l}$, we observe that $X_0^l, X_1^l, \ldots, X_{k-1}^l$ are contained in at most $(p - 1)/l$ distinct residue classes mod $p$. Then, by reading (19) mod $p$, we derive that the elements of $S_3$ are contained in at most $(p - 1)/l$ distinct residue classes mod $p$. Consequently,

$$|S_3| \leq \left(\lfloor z_3/p \rfloor + 1\right)\left(\frac{p-1}{l}\right)$$

which implies (22). \qed

For $\mu_0$ with $0 \leq \mu_0 < k$, we denote by $\nu(A_{\mu_0})$ the number of distinct $\mu$ with $0 \leq \mu < k$ such that $A_\mu = A_{\mu_0}$. We observe that there exists $A_{\mu_0} \in S_3$ such that

$$\nu(A_{\mu_0}) \geq |T_3|/|S_3|$$
where $T_3$ denotes the set of all $\mu$ with $0 \leq \mu < k$ and $A_\mu \in S_3$. Therefore, Lemma 1 gives a lower bound for $v(A_{\mu_0})$. On the other hand, we prove

**LEMMA 2.** Suppose that (1) with $l \geq 3$ is satisfied. Then

$$
v(A_{\mu_0}) \leq 2^{o(d_1)} \left( \left\lceil \frac{k}{A_{\mu_0}} \right\rceil + 1 \right)
$$

for every $\mu_0$ with $0 \leq \mu_0 < k$.

**Proof.** For every $\mu_1$ with $0 \leq \mu_1 < k$ and $A_\mu = A_{\mu_1}$, it suffices to show that the number of $\mu$ with $0 \leq \mu < k$, $A_\mu = A_{\mu_1}$, and $0 \leq \mu - \mu_1 < A_{\mu_1}$ is at most $2^{o(d_1)}$. Let $\mu$ satisfy $0 < \mu - \mu_1 < A_{\mu_1}$ and $A_\mu = A_{\mu_1}$. Then, we derive from (19) and $\gcd(m, d) = 1$ that

$$
\left( \frac{\mu - \mu_1}{A_{\mu_1}} \right) d = \left( X_\mu - X_{\mu_1} \right) \left( \frac{X_\mu^l - X_{\mu_1}^l}{X_\mu - X_{\mu_1}} \right)
$$

where $(\mu - \mu_1)/A_{\mu_1}$ is a positive integer $< l$. For $\mu \neq v$, we put

$$
X_{\mu, v} = \frac{X_\mu^l - X_v^l}{X_\mu - X_v}, \quad X'_{\mu, v} = X_{\mu, v} l^{-\delta}
$$

where $\delta = 0$ if $l \nmid d$ and $\delta = 1$ if $l \mid d$. We observe that every prime factor of $X'_{\mu, v}$ is $\equiv 1 \pmod{l}$. Consequently, $p(X_{\mu, \mu_1}) \geq l$ and

$$
\gcd \left( \frac{\mu - \mu_1}{A_{\mu_1}}, X_{\mu, \mu_1} \right) = 1
$$

which implies that $X_{\mu, \mu_1} \mid d$. Since $X'_{\mu, \mu_1} > 1$ is monotonic increasing in $\mu$ and has $< 2^{o(d_1)}$ divisors, we conclude that the number of $\mu$ with $0 < \mu - \mu_1 < A_{\mu_1}$ and $A_\mu = A_{\mu_1}$ is less than $2^{o(d_1)}$. \qed

As an immediate consequence of Lemma 2, we have

**COROLLARY 2.** Let $\alpha_1 > 0$. Suppose that (1) with

$$
l \geq \alpha_1 k
$$

is satisfied. Then, for every $A_{\mu_0} \in S_1$, we have

$$
v(A_{\mu_0}) \leq c 2^{o(d_1)}
$$

for an effectively computable number $c$ depending only on $\alpha_1$. 

\[ \text{124} \quad \text{T. N. Shorey and R. Tijdeman} \]
For applying Corollary 2, we obtain (24) under certain assumptions in the next three lemmas.

**LEMMA 3.** Let \( \varepsilon > 0 \). There exists an effectively computable number \( c_1 \) depending only on \( \varepsilon \) such that (1) with \( k \geq c_1 \) and \( l > 4\omega(d_1) + 2 \) implies that

\[
l \geq (1-\varepsilon)k \frac{\log \log k}{\log k}.
\]  

(26)

This is (2.11) of [9]. The estimate (26) is slightly weaker than (24). In the next two lemmas, we sharpen (26) to (24) under additional assumptions.

**LEMMA 4.** Let \( \varepsilon > 0 \) and \( \varepsilon_1 > 0 \). Suppose that (1) with \( l > 4\omega(d_1) + 2 \) is satisfied. There exists an effectively computable number \( c_2 \) depending only on \( \varepsilon \) and \( \varepsilon_1 \) such that

\[
l \geq c_2 k 
\]  

or

\[
\varepsilon_1^{-1} \pi(k) < |T| < \varepsilon k.
\]  

(28)

**Proof.** We may assume that \( 0 < \varepsilon < 1/2 \), \( 0 < \varepsilon_1 < 1/2 \) and that \( k \) exceeds a sufficiently large number depending only on \( \varepsilon \) and \( \varepsilon_1 \). We write \( \theta = 4e^{4\varepsilon_1^{-1}} \). Further, we observe from \( l > 4\omega(d_1) + 2 \) that \( l \geq 7 \) and there exists a divisor \( d' \) of \( d_1 \) satisfying

\[
\omega(d') = 1
\]  

(29)

and

\[
d' \geq d_1^{1/\omega(d_1)} \geq d_1^{4^{(t-3)}}
\]

which, together with (2.1) of [9], implies that

\[
d' \geq C_3 d_1^{4^{(1-1/(t-3))}t}
\]  

(30)

where \( C_3 \) is the absolute constant occurring in (2.1) of [9].

First, we assume that

\[
|S_2(\theta)| \geq \frac{\varepsilon k}{2}.
\]
For distinct \( A_\mu \in S_2(\theta) \) and \( A_v \in S_2(\theta) \) with \( \mu > v \), we observe from (19) that
\[
A_\mu X_\mu^l - A_v X_v^l = (\mu - v)d.
\]

Now, we apply the Sieve-theoretic Lemma 1 of Erdős [3] to derive that there exist positive integers \( P, Q \) and \( R \) such that
\[
\max(P, Q, R) \leq c_3, \quad \gcd(P, Q) = 1
\]
and
\[
PX_\mu^l - QX_v^l = Rd =: Nd'
\]
is satisfied by at least \( c_4k \) pairs \( X_\mu, X_v \) where \( c_3, c_4 \) and the subsequent letter \( c_5 \) are effectively computable numbers depending only on \( \epsilon \) and \( \epsilon_1 \). Further, by (30), (2.7) of [9] and \( l \geq 7 \), we observe that
\[
N \leq (d')^{2l/5 - 1}.
\]

Now, we apply Corollary 1(b) of Evertse [5] and (29) to conclude that
\[
c_4k \leq c_5l^{\omega(d')} = c_5l.
\]

Thus, we may assume that
\[
|S_2(\theta)| < \frac{\epsilon k}{2}.
\]
(31)

First, we consider the case that \( |T| \geq \epsilon k \). Then, we derive from (31) that
\[
|S_1| = |S_2| + |S_1 - S_2| < \frac{\epsilon k}{2} + (1 - \epsilon)k = \left(1 - \frac{\epsilon}{2}\right)k.
\]

Now, we apply Lemma 8 of [9] with \( f(k) = (\epsilon \log k)/4 \) and a divisor \( d' \) of \( d \) satisfying (29) and (30). In view of (30) and (2.7) of [9], we see that assumption (4.28) of [9] is satisfied. Hence, we conclude that
\[
l \geq (1 - \epsilon) \frac{\epsilon k}{4}.
\]

Consequently, it remains to consider the case \( |T| \leq \epsilon_1^{-1} \pi(k) \). Note that \( v(A_\mu) = 1 \) if \( A_\mu \geq k \). We apply Lemma 5 of [9] and Lemma 6 of [9] with \( \gamma = 2\epsilon_1^{-1} \).
and \( \eta = 1/2 \) to derive that there exists a subset \( S_4 \) of \( S_2(\theta) \) satisfying \( |S_4| \geq k/4 \). Hence, we conclude from (31) that

\[
\frac{k}{4} \leq |S_4| \leq |S_2(\theta)| < \frac{ek}{2}
\]

which is not possible. Hence, (27) or (28) is valid. \( \square \)

Now, we derive from Lemma 1 and Lemma 4 the following result.

**Lemma 5.** Suppose that (1) with \( l > 4\omega(d_1) + 2 \) is satisfied. There exists an effectively computable absolute constant \( c_6 > 0 \) such that, for \( k \geq c_6 \),

\[
l \geq c_6^{-1}k \quad \text{and} \quad |T| \geq \frac{k}{32}
\]  \( (32) \)

or

\[
p(d_1) \geq lk/5.
\]  \( (33) \)

**Proof.** Let \( \varepsilon = 1/32 \). We refer to Lemma 4 with \( \varepsilon = \varepsilon_1 = 1/32 \) to conclude that we may assume that \( |T| < \varepsilon k \). Then, we apply Lemmas 5 and 6 of [9] with \( g = 2\varepsilon \log k \) and \( \eta = 16\varepsilon \) to derive that there exists a subset \( S_5 \) of \( S_2(k^{1+4\varepsilon}) \) satisfying \( |S_5| \geq 8\varepsilon k \). Now, we apply Lemma 1 with \( S_3 = S_5 \) to derive that

\[8\varepsilon k \leq |S_5| \leq (k^{1+4\varepsilon} + p - 1)/l\]

which, together with (26), implies (33). \( \square \)

In the above lemmas, we have considered (1) under the assumption \( l > 4\omega(d_1) + 2 \). On the other hand, if \( l \leq 4\omega(d_1) + 2 \), we show that \( \omega(d_1) \) is so large that (3), (4) and (5) follow immediately.

**Lemma 6.** Let \( \varepsilon > 0 \). There exist effectively computable numbers \( c_7 \) and \( c_8 > 0 \) depending only on \( \varepsilon \) such that (1) with \( k \geq c_7 \) and \( l \leq 4\omega(d_1) + 2 \) implies that

\[
(\tau(\varepsilon))^{\omega(d_1)} > k^{1+c_8} \quad \text{if} \ l \geq 7
\]  \( (34) \)

and

\[
(\tau(\varepsilon))^{\omega(d)} > k^{1+c_8} \quad \text{if} \ l \in \{2, 3, 5\}.
\]  \( (35) \)

**Proof.** If \( l \leq 30 \), then (34) and (35) follow immediately from Corollary 1 of [9]. Thus we may assume \( l > 30 \). Now we apply Lemma 1 of [10]. It is easy to check
that its proof remains valid if the condition that \( m, m + d, \ldots, m + (k - 1)d \) are all \( l \)th perfect powers is replaced by condition (1) of the present paper. Thus inequality (13) of [10] holds which implies

\[
(\tau(\varepsilon))^{\omega(d)} \geq 21.5 \log k > k^{1.03}.
\]

In addition to the above lemmas, the proof of Theorem 3 depends on the next three lemmas. We start with a version of Lemma 1 of Erdős [3]. The proof depends on Brun’s Sieve method.

**Lemma 7.** Let \( \varepsilon > 0 \) and \( x \geq 3 \). For a positive integer \( r \), we write \( E_r(x) \) for a set \( \{a_1 < a_2 < \cdots < a_r\} \) of \( r \) positive integers not exceeding \( x \). There exist effectively computable numbers \( x_0 \) and \( \beta \) depending only on \( \varepsilon \) such that for \( x \geq x_0 \) and \( r \geq \beta x/\log x \), we can find \( \beta x/4 \log x \) pairs \( a_i, a_j \) with \( i > j \) satisfying

\[
\gcd(a_i, a_j) \geq x^{1-\varepsilon}.
\]

If \( 0 < \beta < 1 \), we can take \( E_r(x) \) the set of all primes not exceeding \( x \) to observe that the assertion of Lemma 7 is no more valid.

**Proof.** We may assume that \( 0 < \varepsilon < 1 \) and \( x_0 \) is sufficiently large. Let \( b_1, \ldots, b_s \) be the set of all integers between \( x^{1-\varepsilon} \) and \( x \) such that every proper divisor of \( b_i \) is less than or equal to \( x^{1-\varepsilon} \). For \( b_i > x^{1-\varepsilon/2} \) and a prime \( p' \) dividing \( b_i \),

\[
x^{1-\varepsilon/2} < b_i \leq p' x^{1-\varepsilon}
\]

which implies that \( p' > x^{\varepsilon/2} \). Therefore, we apply Brun’s Sieve to conclude that

\[
s \leq x^{1-\varepsilon/2} + c_{10} \varepsilon^{-1} x/\log x \leq 2c_{10} \varepsilon^{-1} x/\log x
\]

where \( c_{10} \) is an effectively computable absolute constant. Further, we observe that every integer between \( x^{1-\varepsilon} \) and \( x \) is divisible by at least one \( b_i \). For every \( b_i \) with \( 1 \leq i \leq s \), we take some \( F(b_i) \in E_r(x) \), if it exists, such that \( F(b_i) \) is divisible by \( b_i \). We denote by \( E'_r(x) \) the set obtained by deleting from \( E_r(x) \) all \( F(b_i) \) with \( 1 \leq i \leq s \). Further, we write \( E''_r(x) \) for the set obtained by deleting from \( E'_r(x) \) all the elements \( \leq x^{1-\varepsilon} \). Observe that

\[
|E''_r(x)| \geq r - x^{1-\varepsilon} - 2c_{10} \varepsilon^{-1} x/\log x.
\]

We take \( \beta = 4c_{10} \varepsilon^{-1} \). Then

\[
|E''_r(x)| \geq \beta x/(4 \log x).
\]
For \( y \in E''(x) \), there exists an \( i \) with \( 1 \leq i \leq s \) such that \( y \) is divisible by \( b_i \) and hence,

\[
\text{gcd}(y, F(b_i)) \geq b_i > x^{1-\varepsilon}.
\]

Now, we derive from Lemma 7 another estimate for \( v(A_{\mu_0}) \) which does not depend on \( \omega(d_1) \) and which includes Corollary 2 of [10]. Compare this estimate with (23) and (25). The proof depends on (2), (16) and a theorem of Evertse [5].

**LEMMA 8.** Suppose that (1) with \( l \geq 3 \) is satisfied. Further, assume that \( m_1 = 1 \).
There exist effectively computable absolute constants \( c_{11} \) and \( c_{12} \) such that for \( k \geq c_{11} \), we have

\[
v(A_{\mu_0}) \leq c_{12} k/\log k
\]

for every \( A_{\mu_0} \in S_1 \).

**Proof.** Let \( \varepsilon = 1/8 \). We may assume that \( c_{11} \) is sufficiently large. We put

\[
t = \lfloor \beta k/\log k \rfloor
\]

where \( \beta \) is the constant appearing in Lemma 7 and we assume that there exist \( 0 \leq \mu_0 < \mu_1 < \cdots < \mu_r < k \) satisfying

\[
A_{\mu_0} = A_{\mu_1} = \cdots = A_{\mu_r}
\]

which, by (19), \( \gcd(m, d) = 1 \) and (21), implies that \( A_{\mu_i} < k \) and \( X_{\mu_i} > 1 \) for \( 0 < i \leq t \). For \( i > j \), we observe again from (19) and (37) that

\[
(\mu_j - \mu_i)m = A_{\mu_0}(\mu_j X_{\mu_i}^i - \mu_i X_{\mu_j}^i).
\]

By Lemma 7, there are at least \([t/5]\) pairs \( \mu_i, \mu_j \) with \( i > j \) satisfying

\[
\text{gcd}(\mu_i, \mu_j) \geq k^{1-\varepsilon}.
\]

Therefore, there exist integers \( P_1 > 0, Q_1 > 0 \) and \( R_1 \neq 0 \) satisfying

\[
\max(P_1, Q_1, |R_1|) \leq k^\varepsilon, \quad \text{gcd}(P_1, Q_1) = 1
\]

and

\[
A_{\mu_0}(P_1 X_{\mu_i}^i - Q_1 X_{\mu_j}^i) = R_1 m
\]

is satisfied by at least \( k^{1-4\varepsilon} \) pairs \( X_{\mu_i}, X_{\mu_j} \) with \( i > j \).
Further, we derive from (16) and (2) that there exist effectively computable absolute constants $c_{13} \geq 8$ and $c_{14} > 0$ such that $l \leq c_{13}$ or

$$\log m \geq (\log d)/2 \geq c_{14}(\log k \loglog k)/\logloglog k.$$

First, we suppose that $l > c_{13}$. Then, we apply Theorem 2 of Evertse [5] with $z = R_1$ and $d = m$ to (38). Using that $m_1 = 1$, we obtain

$$k^{1-4\varepsilon} \leq R(l, m) + 2 \leq l + 2.$$

Then, if $l|\gcd(A_{\mu_0}, m)$, we see from (19), (37) and $\gcd(m, d) = 1$ that $l|\mu_i$ for $0 \leq i \leq t$ which implies that $k > lt > k^{2-5\varepsilon}$. Thus $l|\gcd(A_{\mu_0}, m)$. Let $X_{\mu_i}$, $X_{\mu_j}$, and $X_{\mu_i}$, $X_{\mu_j}$ be distinct pairs satisfying (38). Now, we see from (38) that

$$l^{\operatorname{ord}(m)}(X_{\mu_i}^l X_{\mu_j}^l - X_{\mu_i}^l X_{\mu_j}^l)$$

which implies that

$$|X_{\mu_i}^l X_{\mu_j}^l - X_{\mu_i}^l X_{\mu_j}^l| \geq l^{\operatorname{ord}(m)-1}.$$

Further, we put

$$\Delta = (m + \mu_i, d)(m + \mu_j, d) - (m + \mu_j, d)(m + \mu_i, d).$$

Then

$$|\Delta| \geq l^{\operatorname{ord}(m)}(m + d)^{2(l-1)/l}$$

and

$$|\Delta| \leq 2kd(m + (k - 1)d) < 2k^2d(m + d).$$

Consequently, we derive that

$$l^{\operatorname{ord}(m)} < 2k^2d^{2/l} \leq m^{1/2},$$

since $l \geq 9$. Now, we observe that

$$R'_1 = R_1^{l^{\operatorname{ord}(m)}}, \quad m' = m/l^{\operatorname{ord}(m)}$$

satisfy $0 < |R'_1| < m^{3/4}$ and $m' \geq m^{1/2}$ which imply that

$$(m')^{(2l/5) - 1} > m > |R'_1|. $$
Hence, we apply again Theorem 2 of Evertse [5] with \( z = R_1 \) and \( d = m' \) to (38) for concluding that \( k^{1 - 4\varepsilon} \leq R(l, m') + 2 = 3 \), since \( m_1 = 1 \) and \( \gcd(m', l) = 1 \). If \( l \leq c_1 \), we apply Theorem 1 of Evertse [5]. Again using \( m_1 = 1 \), we obtain

\[
k^{1 - 4\varepsilon} \leq 2R(l, |R_1|m) + 6 \leq 2|R(l, |R_1|) + 6 \\
\leq 2^{\log(R_1)+1} + 6 \leq c_{13}^{2\varepsilon} \log k / \log \log k
\]

which is not possible if \( c_1 \) is sufficiently large. \( \square \)

Finally, we apply Lemma 8 and Lemma 1 to conclude the following result.

**Lemma 9.** Suppose that (1) is satisfied. Further, assume that \( l > 4\omega(d_1) + 2 \) and \( m_1 = 1 \). There exist effectively computable absolute constants \( c_{15} \) and \( c_{16} > 0 \) such that for \( k \geq c_1 \), we have

\[
p(d_1) \geq c_{16} k \log k.
\] (39)

**Proof.** Let \( \varepsilon = 1/32 \) and we may assume that \( c_{15} \) is sufficiently large. First, we consider the case that \( |T| \geq \varepsilon k \). Then, we apply Lemma 1 with \( S_3 = S_2 \) and (36) to derive that

\[
\varepsilon k \leq |T| \leq c_{12} \frac{k}{\log k} \left( \frac{k + p - 1}{l} \right)
\]

which, together with (26), implies (39). If \( |T| < \varepsilon k \), we apply Lemma 5 to derive (33). \( \square \)

**Section 3. Proof of Theorem 1**

Let \( \varepsilon_1 = \varepsilon/30 \) and suppose that \( C_2 \) is sufficiently large. In view of (2.12) of [9], we may suppose that \( l \leq 4\omega(d_1) + 2 \). Then, we apply Lemma 6 to derive that

\[
\omega(d_1) \geq \eta'(\varepsilon_1) \log k.
\]

Consequently, we obtain by prime number theory

\[
\log d_1 \geq \sum_{p \leq (1 - \varepsilon_1)\eta'(\varepsilon_1) \log k \log \log k} \log p \geq (1 - \varepsilon_1)^2 \eta'(\varepsilon_1) \log k \log \log k
\]

which implies (3). \( \square \)

**Proof of Theorem 2.** We may suppose that \( C_3 > c_7 \) is sufficiently large. Then, by Lemma 6 and \( p > l \), we may assume that \( l \geq 4\omega(d_1) + 3 \geq 7 \). Now, by
Lemma 5, we may suppose (32). Then, we apply Corollary 2 to conclude that for every $A_{\mu_0} \in S_1$,

$$v(A_{\mu_0}) \leq c_{1,7}2^{\omega(d_1)}$$ \hfill (40)

where $c_{1,7}$ is an effectively computable absolute constant.

We obtain from (32) and (40) that

$$|S_2| \geq [k(32c_{1,7}2^{\omega(d_1)} - 1)] \geq 2c_6,$$ \hfill (41)

where we may suppose the right-hand inequality of (41), otherwise (4) follows immediately from $p > 1$. Finally, we apply Lemma 1 with $S_3 = S_2$ to obtain

$$|S_2| \leq \frac{k + p - 1}{l}$$

which, together with (41) and (32), implies (4). \hfill \Box

**PROOF OF COROLLARY 1.** We may assume that $C_5$ is sufficiently large. For the proof of (6) and (7), we apply Theorem 2 to assume that

$$(\tau(\varepsilon))^{\omega(d_1)} \geq k(\log k)^{-2} \quad \text{if } l \geq 7$$ \hfill (42)

and

$$(\tau(\varepsilon))^{\omega(d)} \geq k(\log k)^{-2} \quad \text{if } l \in \{2, 3, 5\}.$$ \hfill (43)

Now, we apply Brun–Titchmarsh Theorem to derive (6) from (42). Further, we apply Prime Number Theorem to obtain (7) from (43).

Now, we turn to the proof of (8) and (9). In view of Lemma 6, we may assume that $l > 4v(d_1) + 2$. Now, by (26), it suffices to show that

$$Q(d_1) \geq lk^{1-\varepsilon} \quad \text{if } l \geq 7$$ \hfill (44)

and

$$Q(d) \geq lk^{1-\varepsilon} \quad \text{if } l \in \{2, 3, 5\}.$$ \hfill (45)

For this, we refer to Theorem 2 to assume that

$$(\tau(\varepsilon))^{\omega(d_1)} \geq k^{e/2} \quad \text{if } l \geq 7$$
and

\((\tau(\varepsilon))^{\omega(d)} \geq k^{e/2}\) if \(l \in \{2, 3, 5\}\)

which imply (44) and (45).

PROOF OF THEOREM 3. (a) We apply Lemma 5 to assume (32) which implies that \(p > l \geq c_6^{-1}k\). This confirms (12) with \(C_6 = c_6^{-1}\).

(b) We may assume that \(k\) exceeds a sufficiently large effectively computable absolute constant, otherwise (13) follows from \(p > l\). Then, we apply Lemma 9 to assume that \(m_1 > 1\). By reading (19) mod \(q\), we have

\[
\mu d \equiv A_{\mu}X_{\mu}^l(\text{mod } q) \quad \text{for } 0 \leq \mu < k.
\]

Since \(q \equiv 1(\text{mod } l)\) is a prime number, we see that \(X_{\mu}^l, X_{\mu_1}^l, \ldots, X_{\mu_{s-1}}^l\) are contained in at most \((q-1)/l\) residue classes mod \(q\). Let \(A_{\mu_0} \in S_1\) and let \(X(\text{mod } q)\) be a residue class mod \(q\). Let \(0 \leq \mu_0 < \mu_1 \cdots < \mu_{s-1} < k\) satisfy \(A_{\mu_0} = A_{\mu_1} = \cdots = A_{\mu_{s-1}}\) and

\[
\mu_1 d \equiv A_{\mu_1}X(\text{mod } q), \quad 0 \leq i < s.
\]

Then, since \(\gcd(m, d) = 1\),

\[
s \leq \left\lfloor \frac{k}{q} \right\rfloor + 1.
\]

Consequently,

\[
\nu(A_{\mu_0}) \leq \left(\left\lfloor \frac{k}{q} \right\rfloor + 1\right)\frac{(q-1)}{l} \leq \frac{k+q-1}{l}
\]

(46)

for every \(A_{\mu_0} \in S_1\).

Let \(\varepsilon = 1/32\). If \(|T| < \varepsilon k\), we apply Lemma 5 to derive (33). Thus, we may suppose that \(|T| \geq \varepsilon k\). Then, we apply (46) and Lemma 1 with \(S_3 = S_2\) to derive that

\[
\varepsilon k \leq |T| \leq \left(\frac{k+q-1}{l}\right)\left(\frac{k+p-1}{l}\right)
\]

which, together with (26), implies either (13) or (14). 

\(\square\)
PROOF OF THEOREM 4. (a) We may assume $0 < \varepsilon < \frac{1}{3}$ and that $C_{12}$ is sufficiently large. Let $0 \leq \mu_0 < k$ satisfy

$$P = P(m + \mu_0 d) = \min_{0 \leq \mu < k} P(m + \mu d) < k^{1/3 - \varepsilon}.$$  

Now, we apply an estimate of Yu[11] on $p$-adic linear forms in logarithms, as in the proof of Lemma 9 of [9], to conclude that

$$\log m \leq \log(m + \mu_0 d) \leq \sum_{p \in \mathcal{P}} \text{ord}_p(m + \mu_0 d) \log p$$

$$\leq \left( \frac{\log l}{l} \right) (\log d) k^{1 - 2\varepsilon} + \sum_{p \in \mathcal{P}} 6 \log k.$$  

By Corollary 6 of [9], we obtain

$$\sum_{p \in \mathcal{P}} 6 \log k \leq 6P \log k < k^{1/3} < \left( \frac{\log l}{l} \right) (\log d) k^{1 - 2\varepsilon},$$

hence

$$\log m \leq 2 \left( \frac{\log l}{l} \right) (\log d) k^{1 - 2\varepsilon}.$$

By (26), we can secure that $\min(k, l) \geq C_{10}$. The preceding inequality combined with (16) and (26) implies that $k$ is bounded by an effectively computable number depending only on $\varepsilon$.

(b) We may assume that $C_{13}$ is sufficiently large. We suppose that $P(m - d) \leq k$. Let $p_1$ be a prime dividing $(m - d)$. If $p_1 \leq \log k$, we apply an estimate of Yu[11], (16) and (26) as mentioned above, to derive that

$$\text{ord}_{p_1}(m - d) \leq c_{18} \frac{(\log k)^5}{k} (\log m)$$  

(47)

where $c_{18}$ and the subsequent letters $c_{19}, c_{20}, c_{21}$ are effectively computable absolute positive constants. If $p_1 > \log k$, we see that

$$\text{ord}_{p_1}(m - d) \leq \max_{1 \leq i \leq k} \text{ord}_{p_1}(i),$$  

(48)

otherwise, by (26),

$$0 < \text{ord}_{p_1}(m(m + d) \cdots (m + (k - 1)d)) \leq c_{19} \frac{k}{p_1} < l$$
which, since $b = 1$, is not possible. By (47),

$$
\sum_{\substack{p_1 \leq \log k \\ p_1 \mid (m-d)}} \text{ord}_{p_1}(m-d) \log p_1 \leq 2c_{18} \frac{(\log k)^6}{k} (\log m).
$$

Further, we observe from (48) that

$$
\sum_{\substack{p_1 > \log k \\ p_1 \mid (m-d)}} \text{ord}_{p_1}(m-d) \log p_1 \leq \pi(k) \log k \leq 2k,
$$

since $P(m-d) \leq k$. Consequently,

$$
\log(|m-d|) \leq 2c_{18} \frac{(\log k)^6}{k} (\log m) + 2k.
$$

By Lemma 5 of [9], we can find $\mu_1$ and $\mu_2$ with $0 \leq \mu_1 < k$, $0 \leq \mu_2 < k$ and $\mu_1 \neq \mu_2$ such that

$$
A_{\mu_i} \leq k^2 \quad \text{for } i = 1, 2.
$$

Further, we observe

$$(\mu_1 - \mu_2)(m-d) = (\mu_1 + 1)(m + \mu_2d) - (\mu_2 + 1)(m + \mu_1d).$$

Therefore, by (19),

$$
|\mu_1 - \mu_2|(m-d) = |(\mu_1 + 1)A_{\mu_2}X_{\mu_2} - (\mu_2 + 1)A_{\mu_1}X_{\mu_1}|.
$$

Now, we apply an estimate of Baker [1] on linear forms in logarithms to the right-hand side of (50) to conclude that

$$
\log(k \mid m-d\mid) \geq \log m - c_{20}(\log k)^2 \left(\frac{\log l}{l}\right) \log(m+(k-1)d)
$$

which, together with (2.19) of [9], (16) and (26), implies that

$$
\log(k \mid m-d\mid) \geq \log m - \frac{(\log k)^4}{k} (\log m) \geq (\log m)/2.
$$

Now, we combine (49) and (51) to derive that $\log m \leq 8k$. Then, we apply (16) and (2.12) of [9] to conclude that $k \leq c_{21}$ which is not possible if $C_{13}$ is sufficiently large. This contradiction proves (18).
References


