ACTA ARITHMETICA
131.3 (2008)

Arithmetic progressions with common difference divisible by small primes

by

N. Saradha (Mumbai) and R. Tijdeman (Leiden)

1. Introduction. For any integer $n \geq 1$ let $P(n)$ and $p(n)$ denote the greatest prime factor and smallest prime factor of n, respectively. Also let $P(1) = p(1) = 1$. We consider the equation

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

in positive integers $n, k \geq 2$, $d > 1$, $b, y, l \geq 3$ with l prime, $\gcd(n,d) = 1$ and $P(b) \leq k$. We write

$$d = D_1 D_2, \tag{1.2}$$

where D_1 is the maximal divisor of d such that all prime divisors of D_1 are congruent to 1 (mod l). Thus D_1 and D_2 are relatively prime positive integers such that D_2 has no prime divisor which is congruent to 1 (mod l). Shorey [Sh88] proved that (1.1) implies

$$D_1 > 1 \quad \text{if } k \geq C_1, \tag{1.3}$$

where C_1 is a large absolute constant. In [SS01], Saradha and Shorey showed that $C_1 = 4$ suffices. Thus for all $k \geq 4$, there exists a prime $\equiv 1 \pmod{l}$ dividing d. Since $l \geq 3$, this implies that (1.1) has no solution if d is composed of the primes 2, 3, and 5 only. For $k = 3$, Győry [G99] showed that (1.1) with $P(b) < k$ is impossible. Further, from [SS01], it follows that (1.3) holds for (1.1) when $k = 3$ provided 2 or 3 divides d. Shorey and Tijdeman [ST90] sharpened (1.3) to

$$D_1 > C_2 k^{l-2}. \tag{1.4}$$

The constant C_2 turns out to be very small and therefore the above inequality is trivial for small values of k.

2000 *Mathematics Subject Classification*: Primary 11D61.

Key words and phrases: arithmetic progression, perfect powers, multiplicative covering.

In [SS01], estimates for D_1 which were non-trivial even for small values of k were given. For example, it was shown that

$$D_1 > 1.59\theta k^{l/2-3.15} \quad \text{for } l \geq 17, \tag{1.5}$$

where

$$\theta = \begin{cases} 1 & \text{if } l \nmid d, \\ 1/l & \text{if } l \mid d. \end{cases} \tag{1.6}$$

The reduction in the exponent of k from $l-2$ in (1.4) to $l/2-3.15$ in (1.5) is due to using a counting argument of Erdős and Selfridge while covering small values of k (see [SS01, Lemma 9]). When $k \geq 11380$, it was shown in [SS01, Lemma 7] that

$$D_1 > \theta k^{l-3+1/l}. \tag{1.7}$$

The proof of this inequality depends on a graph-theoretic argument due to Erdős and Selfridge [ES75] and some further refinements in [Sa97]. In this paper, we improve this graph-theoretic argument (see Lemma 4.2). Using this improvement we show

THEOREM 1.1. *Let* (1.1) *hold with* $l \geq 5$. *Put*

$$E_1 = \max\left(0.7\theta k^{l-3}, \frac{l\theta}{2k}\, n^{(l-2)/l}\right), \qquad E_2 = \max\left(0.7\theta k^{l-4}, \frac{l\theta}{3k}\, n^{(l-3)/l}\right).$$

(i) *Suppose* $k \geq 4$ *and* d *is divisible by* 2 *or* 3. *Then*

$$D_1 > E_1.$$

(ii) *Suppose* $5 \mid d$. *Then*

$$D_1 > E_1 \quad \text{if } k \geq 8 \text{ or } k = 6 \quad \text{and} \quad D_1 > E_2 \quad \text{if } k = 7.$$

(iii) *Suppose* $7 \mid d$. *Then*

$$D_1 > E_1 \quad \text{if } k \geq 25 \quad \text{and} \quad D_1 > E_2 \quad \text{if } 8 \leq k \leq 24.$$

In [BBGH06], it was shown that (1.1) with $4 \leq k \leq 11$ and $P(b) \leq k/2$ has no solution. This result depends on Galois representation theory of modular forms. As an immediate consequence of this result and Theorem 1.1 we get the following corollary.

COROLLARY 1.2. *Let* (1.1) *hold with* $k \geq 4$, $P(b) \leq k/2$ *and* $l \geq 5$. *Then*

(i) $D_1 > E_1$ *if* 2 *or* 3 *or* 5 *divides* d.
(ii) $D_1 > E_2$ *if* $7 \mid d$.

REMARKS. (i) When $l = 3$, it was shown in [SS01, Theorem 3] that

$$D_1 > 0.41\theta k^{1/3}.$$

We do not have any improvement over this.

(ii) Let $k = 3$. As mentioned earlier, (1.1) with $P(b) < 3$ does not hold. Now let $P(b) = 3$. Suppose $2 \mid d$. Then $n(n+d)(n+2d) = 3^\alpha y^l$ for some integer $\alpha > 0$. Hence $(n, n+d, n+2d) = (3^\alpha y_1^l, y_2^l, y_3^l)$ or $(y_1^l, 3^\alpha y_2^l, y_3^l)$ or $(y_1^l, y_2^l, 3^\alpha y_3^l)$ for some positive integers y_1, y_2 and y_3. Thus

$$y_3^l - y_2^l = d \quad \text{or} \quad y_3^l - y_1^l = 2d \quad \text{or} \quad y_2^l - y_1^l = d.$$

Now we see that (1.3) holds since the difference of two lth powers is always divisible by a prime congruent to 1 (mod l). Note that $3 \nmid d$ since $\gcd(n, d) = 1$. It is still not known if (1.3) holds in the remaining case of d odd and $3 \nmid d$.

(iii) The constant 0.7 in the definitions of E_1 and E_2 is obtained from [SS01, Lemma 5] by taking $\kappa = 7$, $l \geq 5$ and $l' = 2, 3$.

2. Basic lemmas

LEMMA 2.1 ([SS01, Lemma 1]). *For $0 \leq i < k$, let $n + id = a_i a_i'$, where a_i is a positive integer with $P(a_i) \leq k$ for $0 \leq i < k$. Let $S = \{a_0, \ldots, a_{k-1}\}$. For every prime $p \leq k$ with* $\gcd(p, d) = 1$, *choose $a_{i_p} \in S$ such that p does not appear to a higher power in the factorization of any other element of S. Let S_1 be the subset of S obtained by deleting from S all a_{i_p} with $p \leq k$ and* $\gcd(p, d) = 1$. *Then*

$$\prod_{a_i \in S_1} a_i \leq (k-1)! \prod_{p \mid d} p^{-\mathrm{ord}_p (k-1)!}. \tag{2.1}$$

Next we combine [SS05, Lemma 10] and [SS01, Lemma 5] to get

LEMMA 2.2. *Assume that* (1.1) *holds.*

(i) *If*

$$D_1 \leq \min\left(0.7\theta k^{l-3}, \frac{l\theta}{2k} n^{(l-2)/l}\right), \tag{2.2}$$

then the products $a_{i_1} a_{i_2}$ with $0 \leq i_1 \leq i_2 < k$ are all distinct.

(ii) *If*

$$D_1 \leq \min\left(0.7\theta k^{l-4}, \frac{l\theta}{3k} n^{(l-3)/l}\right), \tag{2.3}$$

then the products $a_{i_1} a_{i_2} a_{i_3}$ with $0 \leq i_1 \leq i_2 \leq i_3 < k$ are all distinct.

We assume (2.2) or (2.3) according to the situation we consider. Under these assumptions a_i's are distinct.

We need to count the number of a_i's composed of certain primes. Several counting functions have been used earlier. See [Sa97], [SS01] and [SS05]. Let $2 = p_1 < p_2 < \cdots$ be the sequence of all primes and $q_1 < q_2 < \cdots$ be the sequence of primes coprime to d. Let $\pi(k)$ and $\pi_d(k)$ denote the number of primes $\leq k$ and the number of primes $\leq k$ which are coprime to d, respectively. Let $C(k,m,\alpha_1,\dots,\alpha_m,r_1,\dots,r_h)$ denote the number of a_r's not divisible by $q_i^{\alpha_i+1}$ for $1\le i\le m$, not divisible by the primes $q_{m+1},\dots,$ and not by certain integers $r_1,\dots,r_h$. Obviously,

$$C(k,m,\alpha_1,\dots,\alpha_m,r_1,\dots,r_h) \ge k-\sum_{i=1}^{m}\left\lceil\frac{k}{q_i^{\alpha_i+1}}\right\rceil-\sum_{q_m<p\le k}\left\lceil\frac{k}{p}\right\rceil-\sum_{s=1}^{h}\left\lceil\frac{k}{r_s}\right\rceil, \tag{2.4}$$

where $\lceil x\rceil$ denotes the smallest integer greater than or equal to x. For $h=0$, we take the last sum to be 0 and write the function as $C(k,m,\alpha_1,\dots,\alpha_m)$.

3. Sets with distinct products. For any set S, by aS we mean the set $\{ax\mid x\in S\}$. We say that S has *property* P_i if the products $x_1\cdots x_i$ are all distinct for any i-tuple $x_1\le\dots\le x_i$ with $x_j\in S$ for $1\le j\le i$. If S has property P_2, the products xy with $x\le y$, $x,y\in S$, are all distinct. We observe that if S has property P_i for some $i\ge 2$, then S has property P_j for any $j\le i$. Suppose (1.1) holds with (2.2); then the set of a_i's has property P_2, by Lemma 2.2.

LEMMA 3.1. *Let $X\subseteq\{1,a,\dots,a^r\}$ with $r\le 5$ and let $n_1,\beta_1,\dots,\beta_{n_1}$ be positive integers with*

$$Y=\bigcup_{i=1}^{n_1}\beta_iX.$$

Let $S\subseteq Y$ be any subset of Y having property P_2. Let $S_i=\beta_iX\cap S$ for $i=1,\dots,n_1$ and assume $|S_1|\ge|S_2|\ge\cdots$. Then

$$|S|\le\begin{cases}\min\{2n_1+1,n_1+r-1\} & \text{if } |S_1|=3,\\ \min\{2n_1,n_1+r\} & \text{if } |S_1|=2.\end{cases}\tag{3.1}$$

Proof. Let $1\le i\le n_1$. Let t_i be the least non-negative integer such that

$$a^{t_i}\beta_i\in S_i.$$

Put $\gamma_i=a^{t_i}\beta_i$. Then $S_i\subseteq\gamma_i\{1,a,\dots,a^5\}$ and $\gamma_i\in S_i$. Since S has property P_2, each S_i has property P_2. Observe that all the differences of the exponents of a of pairs of elements from some S_i have to be distinct, i.e., there are no non-negative integers $x_1<y_1$ and $x_2<y_2$ with

$$\gamma_{i_1}a^{x_1},\gamma_{i_1}a^{y_1}\in S_{i_1},\quad \gamma_{i_2}a^{x_2},\gamma_{i_2}a^{y_2}\in S_{i_2}\quad\text{and}\quad y_1-x_1=y_2-x_2,\tag{3.2}$$

for some i_1 and i_2 with $1\le i_1,i_2\le n_1$. This is because if (3.2) holds, then

$$\gamma_{i_1}a^{x_1}\cdot\gamma_{i_2}a^{y_2}=\gamma_{i_1}a^{y_1}\cdot\gamma_{i_2}a^{x_2},$$

contradicting property P_2. As $S\subseteq\{1,a,a^2,a^3,a^4,a^5\}$, only the five differences $1,2,3,4,5$ are available. Observe that if $|S_1|=4$ it generates 6 differences, and if $|S_1|=3$ then 3 differences. Hence we obtain $|S_1|\le 3$ and $|S_i|\le 2$ for $i>1$. Thus $|S|\le 2n_1+1$ if $|S_1|=3$ and $|S|\le 2n_1$ if $|S_1|\le 2$.

Moreover, if $S=\{1,a,a^2,\dots,a^r\}$, then the number of sets S_i with $|S_i|=2$ is at most $r-3$ if $|S_1|=3$ and at most r if $|S_1|=2$. Thus

$$|S|\le 3+2(r-3)+(n_1-r+2)=n_1+r-1$$

if $|S_1|=3$, and otherwise

$$|S|\le 2r+n_1-r=n_1+r. \ \blacksquare$$

LEMMA 3.2. *Let $X\subseteq\{1,a,\dots,a^r\}$ with $r\le 5$ and let $n_1,\beta_1,\dots,\beta_{n_1}$ be positive integers with*

$$Y=\bigcup_{i=1}^{n_1}\beta_i X.$$

Let $S\subseteq Y$ be any subset of Y having property P_3. Let $S_i=\beta_i X\cap S$ for $i=1,\dots,n_1$ and assume $|S_1|\ge|S_2|\ge\cdots$. Then

$$|S|\le\begin{cases} n_1+3 & \text{if } X\subseteq\{1,a,a^2,a^3,a^4,a^5\},\\ n_1+2 & \text{if } X\subseteq\{1,a,a^2,a^3,a^4\},\\ n_1+1 & \text{if } X\subseteq\{1,a,a^2\}.\end{cases}\tag{3.3}$$

Proof. As seen in Lemma 3.1, there exists γ_i such that $S_i\subseteq\gamma_i\{1,a,\dots,a^5\}$ and $\gamma_i\in S_i$ and

$$|S_1|\le 3\quad\text{and}\quad |S_i|\le 2\quad\text{for } i>1.$$

Also, there are no positive integers x_1,y_1 and x_2,y_2 for which (3.2) holds for any i_1,i_2 with $1\le i_1,i_2\le n_1$. Further, property P_3 implies that there are no positive integers x, y and z with $\gamma_{i_1}a^x\in S_{i_1}$, $\gamma_{i_2}a^y\in S_{i_2}$, $\gamma_{i_3}a^z\in S_{i_3}$ for some i_1,i_2,i_3 with $1\le i_1,i_2,i_3\le n_1$ such that

$$x+y=z\quad\text{or}\quad x=2y.$$

Suppose the first possibility occurs; then

$$(\gamma_{i_1}a^x)(\gamma_{i_2}a^y)(\gamma_{i_3})=(\gamma_{i_1})(\gamma_{i_2})(\gamma_{i_3}a^z),$$

contradicting P_3. Suppose the second possibility occurs; then,

$$(\gamma_{i_1}a^x)(\gamma_{i_2})^2=(\gamma_{i_1})(\gamma_{i_2}a^y)^2,$$

again contradicting P_3. Using the above observations we find that if $|S_1|=3$, then $|S_i|\le 1$ for $i\ge 2$, giving $|S|\le n_1+2$. This can only happen if $r>2$. Let $|S_1|=2$. In this case if $X\subseteq\{1,a,a^2,a^3,a^4\}$, then $|S_i|\le 1$ for $i\ge 2$. If $X\subseteq\{1,a,a^2,a^3,a^4,a^5\}$, then $|S_3|\le|S_2|\le 2$ and $|S_i|\le 1$ for $i\ge 4$. The lemma follows. $\blacksquare$

4. Lemmas based on graph theory. Let $X\ge 1$ and $S\subseteq[1,X]$ be a set of integers. Let U and V be such that every integer in S can be expressed as uv with $u\in U$ and $v\in V$. We call such a pair of sets (U,V) a *multiplicative covering* for S. This construction was first given in [ES75] when $S = [1, X]$ and it was refined in [Sa97, p. 157]. Let $i \geq 1$ be an integer. In the lemma below we construct a multiplicative covering (U, V) for a set S of integers not divisible by some given prime.

LEMMA 4.1. *Let $i \geq 1$ be an integer and S be the set of positive integers $\leq X$ not divisible by p_i. Take integers $m \geq 1$ and $T \geq 1$. Let $U = U(m, T)$ denote the set of integers $< T$ composed of $p_1, \ldots, p_m$ and not divisible by p_i. With every prime p_j, $j \neq i$, let the integer $r_j(T)$ denote the smallest integer $\geq T$ not divisible by p_i with $P(r_j(T)) = p_j$. Define*

$$V_j = \{w \mid w \leq p_j X / r_j(T),\ p(w) = p_j \text{ and } p_i \nmid w \text{ for } 1 \leq j \leq m\},$$
$$V_{m+1} = \{w \mid w \leq X,\ w = 1 \text{ or } p(w) \geq p_{m+1} \text{ and } p_i \nmid w\}.$$

Put

$$V = \bigcup_{j=1}^{m+1} V_j.$$

(Note that $V_i = \emptyset$ if $i \leq m$.) Then

$$|V| = \sum_{j=1,\, j\neq i}^{m+1} \left(\frac{\varphi(p_1 \cdots p_{j-1} p_i^{(j)})}{p_1 \cdots p_{j-1} p_i^{(j)}} \frac{X}{r_j(T)} + E_j \right)$$

where for $1 \leq j \leq m+1, j \neq i$, we define

$$p_i^{(j)} = \begin{cases} p_i & \text{if } j < i \leq m \text{ or } m < i, \\ 1 & \text{otherwise}, \end{cases}$$

and

$$E_j \leq \max \left\{ \varrho(z) - \frac{\varphi(p_1 \cdots p_{j-1} p_i^{(j)}) z}{p_1 \cdots p_{j-1} p_i^{(j)}} \right\},$$

where $\varrho(z)$ is the number of integers $\leq z$ and coprime to $p_1, \ldots, p_{j-1}, p_i^{(j)}$ and the maximum is taken over all z with $0 \leq z < p_1 \cdots p_{j-1} p_i^{(j)}$ and $\gcd(z, p_1 \cdots p_{j-1} p_i^{(j)}) = 1$.

We refer to [Sa97] for the above construction. The fact that such a pair (U, V) is a multiplicative covering for S can be easily checked.

The following is a refinement of Lemma 3 of [ES75] which depends on graph theory. Let R be a given set of integers having property P_2, i.e. all products $r_1 r_2$ with $r_1 \leq r_2$ and $r_1, r_2 \in R$ are distinct. Let (U, V) be a multiplicative covering for $[1, X]$. We draw a bipartite graph $G_R = G_R(U, V)$ as follows. The vertices of the bipartite graph are the integers in U and the integers in V. We draw an edge between a vertex $u \in U$ and a vertex $v \in V$ if uv equals an integer $r \in R$. Since R satisfies P_2, the graph G_R contains no rectangle. In [ES75], it was shown that E_R, the number of edges in G_R, satisfies

$$E_R \le |V| + \binom{|U|}{2}.$$

We improve the inequality as follows.

LEMMA 4.2. *Let R be a set of integers having property P_2. Let G_R be the graph drawn as above. Then*

$$E_R \le |V| + |W(U)|,$$

where $W(U)$ is the set of ratios > 1 of pairs of integers from U.

REMARK 4.3. Obviously we have $|W(U)| \le \binom{|U|}{2}$, but in our applications $|W(U)|$ is much smaller than $\binom{|U|}{2}$.

REMARK 4.4. By using Lemma 3 of [ES75], it has been shown in [Sa97] that (1.1) implies that $k \le 11380$ as compared to ≤ 30000 obtained in [ES75]. It is clear that the improvement obtained in Lemma 4.2 will further reduce the bound for k.

Proof of Lemma 4.2. We follow the proof of [ES75]. If a pair of edges emanate from the same vertex, we call the pair a *concurrent pair*. For $i \ge 1$, let s_i denote the number of vertices in V from which i edges emanate. Then

$$E_R = \sum_{i\ge1} is_i = \sum_{i\ge1} s_i + \sum_{i\ge2}(i-1)s_i \le |V| + \sum_{i\ge2}\binom{i}{2}s_i.$$

Let us consider a vertex $v \in V$ from which i edges emanate. The number of concurrent pairs is $\binom{i}{2}$. Thus the total number of concurrent pairs in the graph is

$$\sum_{i\ge2}\binom{i}{2}s_i.$$

Let u_1, u_1', u_2, u_2' be elements of U such that

$$\frac{u_1'}{u_1} = \frac{u_2'}{u_2}.$$

Suppose u_1 and u_1' are the end points of a concurrent pair of edges, as also are u_2 and u_2'. Then there exist $v_1, v_2 \in V$ such that

$$u_1v_1 = r_1, \quad u_1'v_1 = r_2, \quad u_2v_2 = r_3, \quad u_2'v_2 = r_4$$

with $r_1, r_2, r_3, r_4 \in R$. Hence

$$r_1r_4 = u_1v_1u_2'v_2 = u_1'u_2v_1v_2 = r_2r_3,$$

a contradiction. Therefore there can be at most one concurrent pair among the pairs having the same ratio. Thus the number of concurrent pairs is at most $|W(U)|$. Hence

$$\sum_{i\geq 2}\binom{i}{2}s_i \leq |W(U)|.$$

This proves the lemma. ∎

We now specialize R to be the set of a_i's. Under condition (2.2) or (2.3) we see from Lemma 2.2 that R has property P_2 or P_3. We apply Lemmas 4.1 and 4.2 to show

LEMMA 4.5. *Let m, i and T be given positive integers. Suppose the a_j's are not divisible by p_i and are arranged in the increasing order as*

$$b_1 < b_2 < \cdots . \tag{4.1}$$

Suppose further that the a_j's have property P_2. Assume that (U,V) is a multiplicative covering for the set S of all integers in $[1,b_h]$ not divisible by p_i as constructed in Lemma 4.1. Then

$$b_h \geq \alpha(h-\beta) \tag{4.2}$$

where

$$\alpha^{-1} = \sum_{j=1,\, j\neq i}^{m+1} \frac{\varphi(p_1\cdots p_{j-1}p_i^{(j)})}{p_1\cdots p_{j-1}p_i^{(j)}r_j(T)}, \qquad \beta = |W(U)| + \sum_{j=1,\, j\neq i}^{m+1} E_j.$$

Proof. Let R be the set of b_i's. Then the number of b_i's less than or equal to b_h is h. This number does not exceed the number of edges in G_R, since (U,V) is a multiplicative covering for S. Thus by Lemma 4.2,

$$h \leq |V| + |W(U)|.$$

Now the result follows from Lemma 4.1 with $X = b_h$. ∎

We apply Lemma 4.5 when 2, 3, 5 or 7 divides d. Recall $\gcd(n,d)=1$.

LEMMA 4.6. *Let* (1.1) *hold. Suppose that the b_h's have property P_2.*

(i) *Let $2\,|\,d$. Then* (4.2) *holds with*

$$(\alpha,\beta) = (2.571, 2.17), (2.842, 3.17), (3.253, 7.1), (3.349, 8.1).$$

(ii) *Let $p(d)=3$. Then* (4.2) *holds with*

$$(\alpha,\beta) = (2.4, 3.34), (2.666, 4.34), (2.823, 5.34), (2.909, 6.34), (2.953, 7.34).$$

(iii) *Let $p(d)=5$. Then* (4.2) *holds with*

$$(\alpha,\beta) = (1.666, 3.6), (2, 4.6), (2.222, 5.6), (2.352, 6.6), (2.769, 10.54), (3.185, 18.54), (3.262, 20.54), (3.534, 36).$$

(iv) *Let $p(d)=7$. Then* (4.2) *holds with*

$$(\alpha,\beta) = (1.867, 3.27), (2.074, 4.72), (2.196, 5.72), (2.263, 6.72), (2.584, 10.86), (2.973, 18.86), (3.407, 38.52).$$

Proof. We need only specify the parameters m and T. Then U is the set of positive integers composed of $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_m$ and V is constructed as in Lemma 4.1. The numbers α, β are computed from Lemma 4.5.

(i) Let $2 \mid d$. Take $i = 1$ and $(m, T) = (2, 9), (2, 27), (3, 15), (3, 25)$, respectively.

(ii) Let $p(d) = 3$. Take $i = 2$ and $(m, T) = (1, 8), (1, 16), (1, 32), (1, 64), (1, 128)$, respectively.

(iii) Let $p(d) = 5$. Take $i = 3$ and $(m, T) = (1, 8), (1, 16), (1, 32), (1, 64), (2, 9), (2, 18), (2, 27), (4, 21)$, respectively.

(iv) Let $p(d) = 7$. Take $i = 4$ and $(m, T) = (1, 8), (1, 16), (1, 32), (1, 64), (2, 9), (2, 18), (3, 18)$, respectively. ∎

5. Application of Lemma 2.1. Inequality (2.1) proves to be basic in the problems of perfect powers in arithmetic progression, as is evident from the papers [Sa97], [SS01] and several other papers by Laishram, Mukhopadhyaya and Shorey. We refer to the survey article [Sh06] of Shorey for these references. We apply in (2.1) the lower estimates for b_h obtained in Lemma 4.6 to get

LEMMA 5.1. *Suppose* (1.1) *holds with* (2.2).

(i) *The case* $p(d) = 2$ *cannot occur.*
(ii) *Let* $p(d) = 3$. *Then* $k \le 124$.
(iii) *Let* $p(d) = 5$. *Then* $k \le 374$.
(iv) *Let* $p(d) = 7$. *Then* $k \le 538$.

Proof. We see from Lemma 2.1 that

$$|S_1| \ge k - \pi_d(k).$$

Since the a_i's satisfy P_1, we get

$$\prod_{a_i \in S_1} a_i \ge \prod_{i=1}^{k-\pi_d(k)} b_i.$$

Hence, by Lemma 2.1,

$$\prod_{i=1}^{k-\pi_d(k)} b_i \le (k-1)! \prod_{p \mid d} p^{-\mathrm{ord}_p (k-1)!}. \tag{5.1}$$

(i) Let $2 \mid d$. Then

$$\prod_{i=1}^{k-\pi(k)+1} b_i \le \prod_{i=1}^{k-\pi_d(k)} b_i \le (k-1)!/2^{\mathrm{ord}_2 (k-1)!}.$$

Put

$$\delta_h = \begin{cases} 2h-1 & \text{for } h \le 8, \\ 2.571(h-2.17) & \text{for } 9 \le h \le 12, \\ 2.842(h-3.17) & \text{for } 13 \le h \le 34, \\ 3.253(h-7.1) & \text{for } 35 \le h \le 41, \\ 3.349(h-8.1) & \text{for } h \ge 42. \end{cases} \tag{5.2}$$

Then by Lemma 4.6(i) we get, for every k,

$$\prod_{h=1}^{k-\pi(k)+1} \delta_h \le (k-1)!/2^{\mathrm{ord}_2(k-1)!}.$$

As is standard now, we first bound k using approximate values of $\pi(k)$ and $(k-1)!$. For the remaining finite number of values of k, we check that the above inequality is not valid.

The proofs for (ii), (iii), and (iv) are similar. For the initial values of δ_h we take the hth positive integer not divisible by p_i. For the other values of h we choose the largest values of $\alpha(h-\beta)$ for (α, β) given in Lemma 4.6(ii), (iii), (iv), respectively. ■

6. Proof of the theorem. (i) Let $2 \mid d$. Then the assertion follows immediately from Lemma 4.6(i).

Now suppose $p(d) = 3$. By Lemma 5.1(ii) we obtain $k \le 124$. We apply (2.4) with $m = 3$, $q_1 = 2$, $q_2 = 5$, $q_3 = 7$, $\alpha_1 = 4$, $\alpha_2 = \alpha_3 = 1$, $h = 1$, $r_1 = 5 \cdot 7$, i.e., we estimate from below the number of a_i's composed of 2, 5 and 7 with their powers not exceeding 4, 1, 1 and not divisible by 35. This yields

$$C(k, 3, 4, 1, 1, 5 \cdot 7) \ge 8 \quad \text{for } 16 \le k \le 124. \tag{6.1}$$

For any k, we denote by $S(k) = S(k, \beta_1, \ldots, \beta_{n_1}, X)$ the set of a_i's $\subseteq Y$ where $X, Y, \beta_1, \ldots, \beta_{n_1}$ are as in Lemma 3.1. In the notation of Lemma 3.1, we take $X = \{1, 2, 2^2, 2^3, 2^4\}$, with $r = 4$ and $n_1 = 3$, $\{\beta_1, \beta_2, \beta_3\} = \{1, 5, 7\}$. By (6.1), we get

$$|S(k)| \ge 8 > n_1 + r,$$

a contradiction to Lemma 3.1.

Now we consider $4 \le k \le 15$. We take $m = 1$, $q_1 = 2$, $\alpha_1 = 2$, $h = 0$ to find

$$C(k, 1, 2) \ge 3.$$

This means that there are at least three a_i's belonging to $\{1, 2, 2^2\}$. Since a_i's are distinct this means property P_2 is not satisfied.

(ii) Let $p(d) = 5$. By Lemma 5.1(iii), we have $k \le 374$.

Let $65 \le k \le 374$. Take $X = \{1, 2, 2^2, 2^3, 2^4, 2^5\}$, $n_1 = 15$,

$$\{\beta_1, \ldots, \beta_{15}\} = \{1, 3, 7, 11, 13, 3 \cdot 7, 3 \cdot 11, 3 \cdot 13, 7 \cdot 11, 7 \cdot 13, \\ 11 \cdot 13, 3^2, 3^2 \cdot 7, 3^2 \cdot 11, 3^2 \cdot 13\}.$$

We apply (2.4) with $m = 5$, $q_1 = 2$, $q_2 = 3$, $q_3 = 7$, $q_4 = 11$, $q_5 = 13$, $\alpha_1 = 5$, $\alpha_2 = 2$, $\alpha_3 = \alpha_4 = \alpha_5 = 1$, $h = 4$, $r_1 = 3 \cdot 7 \cdot 11$, $r_2 = 3 \cdot 7 \cdot 13$, $r_3 = 3 \cdot 11 \cdot 13$, $r_4 = 7 \cdot 11 \cdot 13$ to get

$$|S(k)| \ge 21.$$

This contradicts Lemma 3.1 with $r = 5$.

For $25 \le k \le 64$, take $X = \{1, 2, 2^2, 2^3, 2^4\}$, $n_1 = 4$, $\{\beta_1, \beta_2, \beta_3, \beta_4\} = \{1, 3, 3^2, 7\}$. Apply (2.4) with $m = 3$, $q_1 = 2$, $q_2 = 3$, $q_3 = 7$, $\alpha_1 = 4$, $\alpha_2 = 2$, $\alpha_3 = 1$, $h = 1$, $r_1 = 3 \cdot 7$ to get

$$|S(k)| \ge 9,$$

contradicting Lemma 3.1 with $r = 4$.

Let $9 \le k \le 24$. Take $X = \{1, 2, 2^2, 2^3\}$, $n_1 = 2$, $\{\beta_1, \beta_2\} = \{1, 3\}$. Apply (2.4) with $m = 2$, $q_1 = 2$, $q_2 = 3$, $\alpha_1 = 3$, $\alpha_2 = 1$, $h = 0$ to get

$$|S(k)| \ge 5,$$

except for $k = 19, 20, 23, 24$ in which cases $|S(k)| \ge 4$. By Lemma 3.1,we have $|S(k)| \le 4$ $(= 2n_1)$. Thus we need to consider $k = 19, 20, 23, 24$ with $|S(k)| = 4$. Let $k = 24$. Then 23 divides a_0, a_{23}; 7 divides a_1, a_8, a_{15}, a_{22}; 19 divides a_2, a_{21}; and 17 divides a_3, a_{20}. Then 16 divides one of $a_0, a_1, a_2, a_3, a_{20}, a_{21}, a_{22}, a_{23}$. Thus the number of a_i's divisible by 16 and not by the primes 7, 17, 19 and 23 is at most 1. Hence $|S(k)| \ge 5$, a contradiction. We give for other values of k the combination of a_i's divisible by certain primes or 16 or 9, by which $|S(k)| \ge 5$, to get a contradiction.

- $k = 23$: 11 divides a_0, a_{11}, a_{22}, but no distinct placings for 4 multiples of 7.
- $k = 20$: 19 divides a_0, a_{19}; 17 divides a_1, a_{18}; no place for 2 multiples of 16.
- $k = 19$: 9 divides a_0, a_9, a_{18}, no place for 2 multiples of 17.

This proves that $D_1 > E_1$ if $k \ge 9$.

Let $k = 6$. There are at most three multiples of 2 and two multiples of 3 among the a_i's, but they cannot be distinct. Hence at least two a_i's are equal to 1.

Let $k = 8$. If there are two multiples of 7, then 7 divides a_0 and a_7 and we can apply the case $k = 6$ to $a_1, \ldots, a_6$. Otherwise there is at most one multiple of 7, of 8, and of 9. Hence there are at least five a_i's with values in $\{1, 2, 4, 3, 6, 12\}$. But the a_i's are distinct and they cannot assume all the three values from either $\{1, 2, 4\}$ or $\{3, 6, 12\}$. This yields a contradiction.

Let $k = 7$. There is at most one multiple of 7, one multiple of 8 and one multiple of 9. Hence there are at least four a_i's in $\{1, 2, 3, 4, 6, 12\}$. A simple check shows that this cannot happen if P_3 holds.

(iii) Let $p(d) = 7$. By Lemma 5.1(iv), we have $k \leq 538$. As seen in the case $5 \mid d$, we will be applying (2.4) and Lemmas 3.1 and 3.2 with suitable choices of parameters for various ranges of values of k so that the lower bound for $C(k, m, \alpha_1, \ldots, \alpha_m, r_1, \ldots, r_h)$ and the upper bound for $|S(k)|$ contradict each other. We give below the range of k and the choice of the parameters.

(a) $118 \leq k \leq 538$: By (2.4) we have

$$C(k, 5, 5, 4, 2, 1, 1, 3 \cdot 5 \cdot 11, 3^2 5^2, 3 \cdot 5 \cdot 13, 3 \cdot 11 \cdot 13) \geq 35.$$

Now take $X = \{1, 2, 2^2, 2^3, 2^4, 2^5\}$, $Z = \{1, 3, 3^2, 3^3, 3^4\}$, $n_1 = 29$, $\{\beta_1, \ldots, \beta_{29}\} = \{Z, 5Z, 5^2, 3 \cdot 5^2, 11Z, 5 \cdot 11, 5^2 11, 13Z, 5 \cdot 13, 5^2 13, 11 \cdot 13, 5 \cdot 11 \cdot 13, 5^2 \cdot 11 \cdot 13\}$ to get

$$|S(k)| \leq 29 + 5 = 34,$$

by Lemma 3.1, which gives the necessary contradiction.

(b) $36 \leq k \leq 117$: By (2.4) we have $C(k, 3, 4, 3, 1) \geq 13$. Now take $X = \{1, 2, 2^2, 2^3, 2^4\}$, $Z = \{1, 3, 3^2, 3^3\}$, $n_1 = 8$, $\{\beta_1, \ldots, \beta_8\} = \{Z, 5Z\}$. Thus $|S(k)| \leq 8 + 4 = 12$, by Lemma 3.1, which gives a contradiction.

(c) $25 \leq k \leq 35$: By (2.4) we have $C(k, 3, 3, 2, 1) \geq 10$. Now take $X = \{1, 2, 2^2, 2^3\}$, $Z = \{1, 3, 3^2\}$, $n_1 = 6$, $\{\beta_1, \ldots, \beta_6\} = \{Z, 5Z\}$. Thus $|S(k)| \leq 6 + 3 = 9$, by Lemma 3.1, which gives a contradiction.

(d) $15 \leq k \leq 24$: By (2.4) we have $C(k, 2, 4, 2) \geq 6$. Now take $X = \{1, 2, 2^2, 2^3, 2^4\}$, $Z = \{1, 3, 3^2\}$, $n_1 = 3$, $\{\beta_1, \beta_2, \beta_3\} = \{Z\}$. Thus $|S(k)| \leq 5$, by Lemma 3.2, which gives a contradiction.

(e) $8 \leq k \leq 14$: By (2.4) we have $C(k, 2, 2, 1) \geq 4$ if $k = 8, 9, 10$ and $C(k, 2, 2, 1) \geq 3$ if $11 \leq k \leq 14$. Using the argument as in the case $5 \mid d$, $k \in \{19, 20, 23, 24\}$, we can improve this as

$$C(k, 2, 2, 1) \geq 4 \quad \text{if } 11 \leq k \leq 14.$$

Suppose $C(k, 2, 2, 1) = 3$. We give the combination of a_i's divisible by certain primes or 8 or 9 which shows that there is a coincidence among the a_i's.

- $k = 14$: 13 divides a_0, a_{13}; 11 divides a_1, a_{12}; no place for 3 multiples of 5.
- $k = 13$: 11 divides a_0, a_{11}; 5 divides a_2, a_7, a_{12}; 9 divides a_1, a_{10}; or 11 divides a_1, a_{12}; 5 divides a_0, a_5, a_{10}; 9 divides a_2, a_{11}; in both cases no place for 2 multiples of 8.
- $k = 12$: 11 divides a_0, a_{11}; no place for 3 multiples of 5.
- $k = 11$: 5 divides a_0, a_5, a_{10}; no place for 2 multiples of 9.

Thus for $8 \le k \le 14$,

$$|S(k)| \ge 4,$$

a contradiction to Lemma 3.2. ∎

References

[BBGH06] M. A. Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. (3) 92 (2006), 273–306.

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

[G99] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, in: Number Theory and its Applications, S. Kanemitsu and K. Győry (eds.), Kluwer, 1999, 145–156.

[Sa97] N. Saradha, *On perfect powers in products with terms from arithmetic progressions*, Acta Arith. 82 (1997), 147–172.

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

[SS05] —, —, *Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression*, Compos. Math. 141 (2005), 541–560.

[Sh88] T. N. Shorey, *Some exponential diophantine equations*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge Univ. Press, 1988, 352–365.

[Sh06] —, *Diophantine approximations*, *Diophantine equations*, *transcendence and applications*, Indian J. Pure Appl. Math. 37 (2006), 9–39.

[ST90] T. N. Shorey and R. Tijdeman, *Perfect powers in products of terms in an arithmetical progression*, Compos. Math. 75 (1990), 307–344.

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400005, India
E-mail: saradha@math.tifr.res.in

Mathematical Institute
Leiden University
P.O. Box 9512
2300 RA Leiden, Netherlands
E-mail: tijdeman@math.leidenuniv.nl

Received on 24.8.2007
and in revised form on 12.12.2007 (5500)