Publ. Math. Debrecen
68/3-4 (2006), 451–475

An estimate for the length of an arithmetic progression the product of whose terms is almost square

By SHANTA LAISHRAM (Mumbai)

Abstract. Erdős conjectured that

$$n(n+d)\dots(n+(k-1)d)=y^2 \qquad (1)$$

in positive integers n, $k \geq 3$, $d > 1$, y with $\gcd(n,d)=1$, implies that k is bounded by an absolute constant. Shorey and Tijdeman [16] showed that (1) implies that k is bounded by an effectively computable number depending only on $\omega(d)$, the number of distinct prime divisors of d. In this paper, an explicit bound for k in terms of $\omega(d)$ is presented.

1. Introduction

For an integer $x > 1$, we denote by $P(x)$ and $\omega(x)$ the greatest prime factor of x and the number of distinct prime divisors of x, respectively. Further we put $P(1)=1$ and $\omega(1)=0$. Let n, d, k, b, y be positive integers such that b is square free, $d \geq 1$, $k \geq 3$, $P(b) \leq k$ and $\gcd(n,d)=1$. We consider the equation

$$n(n+d)\dots(n+(k-1)d)=by^2 \quad \text{in } n,d,k,b,y \quad \text{with } P(b) \leq k. \qquad (2)$$

Mathematics Subject Classification: Primary: 11D61.
Key words and phrases: arithmetic progressions, diophantine equations, squarefree integers, congruences.
The research partially supported by TIFR Endowment Fund.

For a survey of results on (2), see [16], [4], [14] and [15]. Equation (2) with $d = 1$ has been solved completely in [3] with $P(b) < k$ and in [11] with $P(b) = k$. Therefore we assume from now onwards that $d > 1$. MARSZALEK [7] proved that (2) implies k is bounded by an effectively computable number k_0 depending only on d. In fact the above assertion holds with k_0 depending only on $\omega(d)$. This is due to SHOREY and TIJDEMAN [16], who proved that $2^{\omega(d)} > c\frac{k}{\log k}$ where c is an effectively computable absolute constant. However the bound k_0 is very large. Further (2) with $\omega(d) = 1$ and $k \notin \{3, 5\}$ has been solved completely in [12] and [8]. Therefore we shall always assume that $\omega(d) \geq 2$. In this paper, we give an explicit bound for k in terms of $\omega(d)$ whenever (2) holds.

For $2 \leq \omega(d) \leq 11$, we define $\kappa_0 = \kappa_0(\omega(d))$ as in the table below.

$\omega(d)$	$\kappa_0(d$ even$)$	$\kappa_0(d$ odd$)$	$\omega(d)$	$\kappa_0(d$ even$)$	$\kappa_0(d$ odd$)$
2	500	800	7	2.643×10^5	1.376×10^6
3	700	3400	8	1.172×10^6	6.061×10^6
4	2900	15300	9	5.151×10^6	2.649×10^7
5	13100	69000	10	2.247×10^7	1.149×10^8
6	59000	3.096×10^5	11	9.73×10^7	4.95×10^8

For $\omega(d) \geq 12$, we define $\kappa_0 = \kappa_0(\omega(d))$ as

$$\kappa_0(\omega(d)) = \begin{cases} 2.25\omega(d)4^{\omega(d)} & \text{if } d \text{ is even,} \\ 11\omega(d)4^{\omega(d)} & \text{if } d \text{ is odd.} \end{cases}$$

We prove

Theorem 1. *Equation* (2) *implies that*

$$k < \kappa_0. \tag{3}$$

Theorem 1 is a direct consequence of the following two propositions.

Proposition 2. *Let* $k \geq \kappa_0$. *Then* (2) *implies that*

$$d < 4c_1(k-1)^2, \tag{4}$$

$$n < c_1(k-1)^3 \tag{5}$$

and hence

$$n + (k-1)d < 5c_1(k-1)^3 \tag{6}$$

where

$$c_1 = \begin{cases} \frac{1}{16} & \text{if } d \text{ is odd}, \\ \frac{1}{8} & \text{if } \operatorname{ord}_2(d) = 1, \\ \frac{1}{4} & \text{if } \operatorname{ord}_2(d) \geq 2. \end{cases}$$

Proposition 3. *Let* $k \geq \kappa_0$*. Then* (2) *implies that*

$$n + (k-1)d \geq 2^{\delta} \frac{5}{16} k^3 \tag{7}$$

where

$$\delta = \min\{\operatorname{ord}_2(d), 3\}.$$

2. Notation and preliminaries

From (2), we have

$$n + \mathrm{id} = A_i X_i^2 \tag{8}$$

for $0 \leq i < k$ with $P(A_i) \leq k$ and $(X_i, \prod_{p \leq k} p) = 1$. Also we have

$$n + \mathrm{id} = a_i x_i^2 \tag{9}$$

for $0 \leq i < k$ with a_i squarefree. Since $\gcd(n, d) = 1$, we see that

$$(A_i, d) = (a_i, d) = (X_i, d) = (x_i, d) = 1 \quad \text{for } 0 \leq i < k. \tag{10}$$

Let

$$T = \{i \mid 0 \leq i < k,\ X_i = 1\}, \quad T_1 = \{i \mid 0 \leq i < k,\ X_i \neq 1\}.$$

Note that $X_i > k$ for $i \in T_1$. For $0 \leq i < k$, let

$$\nu(A_i) = |\{j \in T_1,\ A_j = A_i\}|. \tag{11}$$

We always suppose that there exist $i_0 > i_1 > \cdots > i_{\nu(A_i)-1}$ such that $A_{i_0} = A_{i_1} = \cdots = A_{i_{\nu(A_i)-1}}$. Similarly we define

$$R = \{a_i \mid 0 \le i < k\}$$

and

$$\nu(a_i) = \big|\{j \mid 0 \le j < k,\ a_i = a_j\}\big|. \tag{12}$$

Define

$$\rho := \rho(d) = \begin{cases} 1 & \text{if } 3 \nmid d, \\ 3 & \text{if } 3 \mid d. \end{cases} \tag{13}$$

The letter p always denotes a prime number and p_i the i-th prime number. Let $P_1 < P_2 < \ldots$ be odd prime divisors of d. Let $r := r(d) \ge 0$ be the unique integer such that

$$P_1P_2\ldots P_r < (4c_1)^{\frac{1}{3}}(k-1)^{\frac{2}{3}} \text{ but } P_1P_2\ldots P_{r+1} \ge (4c_1)^{\frac{1}{3}}(k-1)^{\frac{2}{3}}. \tag{14}$$

If $r = 0$, we understand that the product $P_1 \ldots P_r = 1$.

Let $d' \mid d$ and $d'' = \frac{d}{d'}$ be such that $\gcd(d', d'') = 1$. We write

$$d'' = d_1d_2,\ \gcd(d_1, d_2) = \begin{cases} 1 & \text{if } \operatorname{ord}_2(d'') \le 1, \\ 2 & \text{if } \operatorname{ord}_2(d'') \ge 2 \end{cases}$$

and we always suppose that d_1 is odd if $\operatorname{ord}_2(d'') = 1$. We call such pairs (d_1, d_2) as partitions of d''.

We observe that the number of partitions of d'' is $2^{\omega(d'')-\theta_1}$ where

$$\theta_1 := \theta_1(d'') = \begin{cases} 1 & \text{if } \operatorname{ord}_2(d'') = 1, 2, \\ 0 & \text{otherwise} \end{cases}$$

and we write θ for $\theta_1(d)$. In particular, by taking $d' = 1$ and $d'' = d$, the number of partitions of d is $2^{\omega(d)-\theta}$.

Suppose that $A_i = A_j$, $i > j$. Then from (8) and (10), we have

$$(i-j)d = A_i(X_i^2 - X_j^2) = A_i(X_i - X_j)(X_i + X_j) \tag{15}$$

such that $\gcd(d, X_i - X_j, X_i + X_j) = 1$ if d is odd and 2 if d is even. Hence for any divisor d'' of d, we have a partition (d_1, d_2) of d'' corresponding to $A_i = A_j$ such that $d_1 \mid (X_i - X_j)$ and $d_2 \mid (X_i + X_j)$ and it is the unique partition of d'' corresponding to the pair (i, j). Similarly, we have unique partition of d'' corresponding to every pair (i, j) whenever $a_i = a_j$.

As in Shorey and Tijdeman [16], the proof depends on comparing an upper bound and a lower bound for $n + (k-1)d$. The upper bound of $n + (k-1)d$ given by Proposition 2 is a consequence of Lemmas 5, 8, 11, 12, 13 which are refinements of results in [16], [1] and [12]. It is proved by counting the number of distinct a_i's and looking at the number of partitions of d. The proof of Proposition 3 is by counting the number of X_i's greater than k and calculating the maximal value of A_i. Proposition 3 is a consequence of Lemmas 4, 6, 7, 9, 10, 14. The new features of the paper are the refinement of the upper bound of the multiplicities of A_i with respect to partitions of d, counting the number of A_i's with multiplicity greater than 1 and the use of r to improve the lower bounds of the maximum of A_i's.

We shall follow the notation of this section throughout the paper. We use Mathematica for the computations in the paper. This is a part of my Master's thesis [6].

3. Lemmas

We begin with some estimates from Prime number theory.

Lemma 1. *We have*

(i) $$\pi(\nu) \le \frac{\nu}{\log \nu}\left(1 + \frac{1.5}{\log \nu}\right) \text{ for } \nu > 1,$$

(ii) $$\pi(\nu) \ge \frac{\nu}{\log \nu}\left(1 + \frac{0.5}{\log \nu}\right) \text{ for } \nu \ge 59,$$

(iii) $$p_i \ge i \log i \text{ for } i \ge 2,$$

(iv) $$\sum_{p \le \nu} \log p < 1.000081\nu \text{ for } \nu > 0,$$

(v) $$\operatorname{ord}_p(k!) \ge \frac{k-p}{p-1} - \frac{\log(k-1)}{\log p} \text{ for } p < k.$$

Proof. The estimates (i), (ii) and (iii) are due to Rosser and Schoenfeld [10]. For estimate (iv), see [13, p. 360] and [2, Prop. 1.7]. For a proof of (v), see [5, Lemma 2(i)]. □

The next result is Stirling's formula, see [9].

Lemma 2. *For a positive integer ν, we have*

$$\sqrt{2\pi\nu}\ e^{-\nu}\nu^{\nu}e^{\frac{1}{2\nu+1}} < \nu! < \sqrt{2\pi\nu}\ e^{-\nu}\nu^{\nu}e^{\frac{1}{12\nu}}.$$

Lemma 3. *Let $\pi_d(k) \le \pi(k) - 1$. Then*

$$|T_1| > k - \frac{(k-1)\log\,(k-1)}{\log\,(n+(k-1)d) - \log 2} - \pi(k). \tag{16}$$

Proof. We use [12, Lemma 3] with $t = k$, $-\log\prod_{p|d} p^{-\operatorname{ord}_p((k-1)!)} \ge 0$ and $\pi_d(k) \le \pi(k) - \omega(d) + 2$. Let $n \ge (k-1)d$. Then $\log n \ge \log(n + (k-1)d) - \log 2$. This with [12, (4.2)] and Lemma 1 (i) gives (16). For $n < (k-1)d$, we have $\log(k-1) + \log d > \log(n+(k-1)d) - \log 2$. This with [12, (4.1)] and Lemma 1 (i) gives (16). □

Lemma 4. *Let $d = d'd''$ with $\gcd(d', d'') = 1$. Let $i_0 \in T_1$ be such that $A_{i_0} \ge d'$. Then*

$$\nu(A_{i_0}) \le 2^{\omega(d'')-\theta_1(d'')}. \tag{17}$$

Proof. For simplicity, we write $\theta_1 = \theta_1(d'')$. Assume that $\nu(A_{i_0}) > 2^{\omega(d'')-\theta_1}$. Then there exists a sequence of indices $i_0 > i_1 > \cdots > i_{2^{\omega(d'')-\theta_1}}$ such that $A_{i_0} = A_{i_1} = \ldots = A_{i_{2^{\omega(d'')-\theta_1}}}$. For each pair (i_0, i_r), $r = 1, 2, \ldots, 2^{\omega(d'')-\theta_1}$, we have a unique partition corresponding to the pair. But there are at most $2^{\omega(d'')-\theta_1}$ partitions of d''. Since $(i_0 - i_r)d = A_{i_0}(X_{i_0} - X_{i_r})(X_{i_0} + X_{i_r})$ and $A_{i_0} \ge d'$, we have

$$\begin{aligned} k > i_0 - i_r &= \frac{A_{i_0}}{d'}\left(\frac{X_{i_0} - X_{i_r}}{d_1}\right)\left(\frac{X_{i_0} + X_{i_r}}{d_2}\right) \\ &\ge \left(\frac{X_{i_0} - X_{i_r}}{d_1}\right)\left(\frac{X_{i_0} + X_{i_r}}{d_2}\right), \end{aligned}$$

where (d_1, d_2) is the partition of d'' corresponding to pair (i_0, i_r). This shows that we cannot have the partition $(\frac{d''}{2^{\theta_1}}, 2^{\theta_1})$ corresponding to any pair. Hence there can be at most $2^{\omega(d'')-\theta_1}-1$ partitions of d'' with respect to $2^{\omega(d'')-\theta_1}$ pairs of (i_0, i_r), $r = 1, \ldots, 2^{\omega(d'')-\theta_1}$. Hence by Box Principle, there exist pairs (i_0, i_r), (i_0, i_s) with $1 \le r < s \le 2^{\omega(d'')-\theta_1}$ and a partition (d_1, d_2) of d'' corresponding to these pairs. Thus

$$d_1 \mid (X_{i_0} - X_{i_r}),\ d_2 \mid (X_{i_0} + X_{i_r}) \text{ and } d_1 \mid (X_{i_0} - X_{i_s}),\ d_2 \mid (X_{i_0} + X_{i_s})$$

so that $\operatorname{lcm}(d_1, d_2) \mid (X_{i_r} - X_{i_s})$. Since $A_{i_r} = A_{i_s} = A_{i_0}$ and $\gcd(d_1, d_2) \le 2$, we have

$$k > (i_r - i_s)\frac{d'}{A_{i_0}} = \frac{(X_{i_r} - X_{i_s})}{\operatorname{lcm}(d_1, d_2)}\frac{(X_{i_r} + X_{i_s})}{\gcd(d_1, d_2)} > \frac{(X_{i_r} + X_{i_s})}{2} > \frac{2k}{2} = k,$$

a contradiction. □

By taking $d' = 1$ and $d'' = d$, the following result is immediate from Lemma 4 since $\theta_1(d) = \theta$.

Corollary 1. *For $i_0 \in T_1$, we have $\nu(A_{i_0}) \le 2^{\omega(d)-\theta}$.*

Lemma 5. *Let $k \ge 17$. Suppose $n \ge c_1(k-1)^3$ or $d \ge 4c_1(k-1)^2$. Then for $0 \le i_0 < k$, we have*

$$\nu(a_{i_0}) \le 2^{\omega(d)-\theta}. \tag{18}$$

Proof. Suppose that $\nu(a_{i_0}) > 2^{\omega(d)-\theta}$. We note that both $x_i + x_j$ and $x_i - x_j$ are even when d is even. Continuing as in the proof of (17) with $d'' = d$, we see that there exists i, j with $i > j$ and

$$k > \frac{a_{i_0}(x_i + x_j)}{2}$$

where $\frac{d}{2} \mid (x_i - x_0)$ if d is even and $d \mid (x_i - x_0)$ if d is odd. We have $x_i \ge x_j + \frac{d}{2}$ so that $k > \frac{1}{2}a_{i_0}(x_i + x_j) \ge \left(a_j x_j^2\right)^{\frac{1}{2}} + \frac{d}{4} \ge n^{\frac{1}{2}} + \frac{d}{4}$ and hence

$$k > \begin{cases} 1 + c_1(k-1)^2 & \text{if } d \ge 4c_1(k-1)^2, \\ (c_1)^{\frac{1}{2}}(k-1)^{\frac{3}{2}} + 1 & \text{if } n \ge c_1(k-1)^3 \end{cases}$$

which is not true for $k \ge 17$. □

Lemma 6. *Equation* (2) *implies that either*

$$d \geq 4c_1(k-1)^2$$

or

$$r \geq \left[\frac{\omega(d)}{3}\right].$$

PROOF. If $r+1 \leq [\frac{\omega(d)}{3}]$, then $\omega(d) \geq 3(r+1)$ giving $d \geq 4c_1(k-1)^2$ by (14). □

Lemma 7. *Let* $S \subseteq \{A_i \mid 0 \leq i < k\}$ *and* $\min_{A_h \in S} A_h \geq U$. *Let* $t \geq 1$. *Assume that*

$$|S| > Q_t \left(\frac{P_1 - 1}{2}\right) \cdots \left(\frac{P_t - 1}{2}\right) \tag{19}$$

where $Q_t \geq 1$ *is an integer. Then*

$$\max_{A_h \in S} A_h \geq 2^\delta Q_t P_1 \ldots P_t + U. \tag{20}$$

PROOF. For an odd $p \mid d$, we have

$$\left(\frac{A_h}{p}\right) = \left(\frac{A_h X_h^2}{p}\right) = \left(\frac{n}{p}\right)$$

where $(\frac{\cdot}{\cdot})$ is Legendre symbol, so that A_h belongs to at most $\frac{p-1}{2}$ distinct residue classes modulo p for each $0 \leq h < k$. If d is even, then A_h also belongs to a unique residue class modulo 2^δ for each $0 \leq h < k$. Hence by Chinese remainder theorem, A_h belongs to at most $\left(\frac{P_1-1}{2}\right) \ldots \left(\frac{P_j-1}{2}\right)$ distinct residue classes modulo $2^\delta P_1 \ldots P_j$ for each j, $1 \leq j \leq t$. Assume that (20) does not hold. Then

$$\max_{A_h \in S} A_h - (U-1) \leq 2^\delta Q_t P_1 \ldots P_t.$$

Therefore

$$|S| \leq \frac{2^\delta Q_t P_1 \ldots P_t}{2^\delta P_1 \ldots P_t} \left(\frac{P_1 - 1}{2}\right) \cdots \left(\frac{P_t - 1}{2}\right),$$

contradicting (19). □

Corollary 2. *Let S and U be as in Lemma 7. Let $|S| \geq s > \left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_t-1}{2}\right)$, then*

$$\max_{A_h \in S} A_h \geq \frac{3}{4} 2^{t+\delta} s + U. \tag{21}$$

Proof. Let $(f-1)\left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_{t-1}-1}{2}\right) < s - Q_t\left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_t-1}{2}\right) \leq f\left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_{t-1}-1}{2}\right)$ where $Q_t \geq 1$ and $1 \leq f \leq \frac{P_t-1}{2}$ is an integer. To see this, write $s = Q\left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_t-1}{2}\right) + Q'\left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_{t-1}-1}{2}\right) + R$ where $0 \leq Q' < \frac{P_t-1}{2}$ and $0 \leq R < \left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_{t-1}-1}{2}\right)$. If $R > 0$, then take $Q_t = Q$, $f-1 = Q'$; if $R = 0$ and $Q' > 0$, then take $Q_t = Q$, $f = Q'$; and if $R = Q' = 0$, then take $Q_t = Q-1$ and $f = \frac{P_t-1}{2}$. We arrange the elements of S in increasing order and let $S' \subseteq S$ be the first $(f-1)\left(\frac{P_1-1}{2}\right)\dots\left(\frac{P_{t-1}-1}{2}\right)+1$ elements and S'' consist of the remaining set. Then we see from Lemma 7 with $t = t-1$ and $Q_t = f-1$ that

$$\max_{A_h \in S'} A_h \geq 2^\delta (f-1) P_1 P_2 \dots P_{t-1} + U = U'.$$

Now we apply Lemma 7 with $U = U'$ in S'' to derive

$$\max_{A_h \in S} A_h \geq 2^\delta Q_t P_1 P_2 \dots P_t + 2^\delta (f-1) P_1 P_2 \dots P_{t-1} + U.$$

Hence to derive (21), it is enough to prove

$$\begin{aligned} &Q_t P_1 \dots P_t + (f-1) P_1 \dots P_{t-1} \\ &\geq \frac{3}{4}\left\{Q_t(P_1-1)\dots(P_t-1) + 2f(P_1-1)\dots(P_{t-1}-1)\right\}. \end{aligned}$$

By observing that

$$Q_t(P_1-1)\dots(P_t-1) \leq Q_t P_1 \dots P_t - Q_t P_1 \dots P_{t-1},$$

$$2f(P_1-1)\dots(P_{t-1}-1) \leq 2f P_1 \dots P_{t-1} - 2f P_1 \dots P_{t-2},$$

it suffices to show that

$$Q_t + \frac{3(Q_t-1)-(2f+1)}{P_t} + \frac{6f}{P_t P_{t-1}} \geq 0$$

which is true since $Q_t \geq 1$ and $1 \leq f \leq \frac{P_t-1}{2}$. $\square$

Lemma 8. *Let s_i denote the i-th squarefree positive integer. Then*

$$s_i \geq 1.6i \quad \text{for} \quad i \geq 78 \tag{22}$$

and

$$\prod_{i=1}^{l} s_i \geq (1.6)^l l! \quad \text{for} \quad l \geq 286. \tag{23}$$

Further let t_i be i-th odd squarefree positive integer. Then

$$t_i \geq 2.4i \quad \text{for} \quad i \geq 51 \tag{24}$$

and

$$\prod_{i=1}^{l} t_i \geq (2.4)^l l! \quad \text{for} \quad l \geq 200. \tag{25}$$

Proof. The proof is similar to that of [12, (6.9)]. For (22) and (24), we check that $s_i \geq 1.6i$ for $78 \leq i \leq 286$ and $t_i \geq 2.4i$ for $51 \leq i \leq 132$, respectively. Further we observe that in a given set of 144 consecutive integers, there are at most 90 squarefree integers and at most 60 odd squarefree integers by deleting multiples of $4, 9, 25, 49, 121$ and $2, 9, 25, 49$, respectively. Then we continue as in the proof of [12, (6.9)] to get (22) and (24). Further we check that (23) holds at $l = 286$ and (25) holds at $l = 200$. Then we use (22) and (24) to obtain (23) and (25), respectively. □

Lemma 9. *Let $X > 1$ be a positive integer. Then*

$$\sum_{i=1}^{X-1} 2^{\omega(i)} \leq \eta(X) X \log X \tag{26}$$

where

$$\eta := \eta(X) = \begin{cases} 1 & \text{if} \quad X = 1, \\ \dfrac{\sum_{i=1}^{X-1} 2^{\omega(i)}}{X \log X} & \text{if} \quad 1 < X < 248, \\ 0.75 & \text{if} \quad X \geq 248. \end{cases} \tag{27}$$

Proof. We check that (26) holds for $1 < X < 11500$. Thus we may assume $X \geq 11500$. Let s_j be the largest squarefree integer $\leq X$. Then by Lemma 8, we have $1.6j \leq s_j \leq X$ so that $j \leq \left[\frac{X}{1.6}\right]$. We have $2^{\omega(i)} = \sum_{e|i} |\mu(e)|$. Therefore

$$\sum_{i=1}^{X-1} 2^{\omega(i)} = \sum_{i=1}^{X-1} \sum_{e|i} |\mu(e)|$$

$$\leq \sum_{1\leq e<X} \left[\frac{X-1}{e}\right] |\mu(e)| \leq (X-1) \sum_{1\leq e<X} \frac{|\mu(e)|}{e} \leq X \sum_{i=1}^{\left[\frac{X}{1.6}\right]} \frac{1}{s_i}.$$

We check that there are 6990 squarefree integers upto 11500. By using (22), we have

$$\begin{aligned}
\sum_{i=1}^{X-1} 2^{\omega(i)} &\leq X \left\{ \sum_{i=1}^{6990} \frac{1}{s_i} - \frac{1}{1.6} \sum_{i=1}^{6990} \frac{1}{i} + \frac{1}{1.6} \sum_{i=1}^{\left[\frac{X}{1.6}\right]} \frac{1}{i} \right\} \\
&\leq X \left\{ \sum_{i=1}^{6990} \frac{1}{s_i} - \frac{1}{1.6} \sum_{i=1}^{6990} \frac{1}{i} + \frac{1}{1.6} \left(1 + \log \frac{X}{1.6}\right) \right\} \\
&\leq \frac{3}{4} X \log X \left\{ \frac{4}{3} \frac{1.1658}{\log X} + \frac{4}{3} \frac{1}{1.6} \right\},
\end{aligned}$$

implying (26). □

Lemma 10. *Let $c > 0$ be such that $c2^{\omega(d)-3} > 1$, $\mu \geq 2$ and*

$$\mathfrak{C}_\mu = \left\{ A_i \;\middle|\; \nu(A_i) = \mu,\ A_i > \frac{\rho 2^\delta k}{3c2^{\omega(d)}} \right\}.$$

Then

$$\begin{aligned}
\mathfrak{C} &:= \sum_{\mu\geq 2} \frac{\mu(\mu-1)}{2} |\mathfrak{C}_\mu| \\
&\leq \frac{c}{8} \eta(c2^{\omega(d)-3}) 2^{\omega(d)} (2^{\omega(d)-\theta} - 1)(\log c2^{\omega(d)-3}).
\end{aligned} \tag{28}$$

Proof. Let $i_1 > i_2 > \cdots > i_\mu$ be such that $A_{i_1} = A_{i_2} = \cdots = A_{i_\mu}$. These give rise to $\frac{\mu(\mu-1)}{2}$ pairs of (i, j), $i > j$ with $A_i = A_j$. Therefore the total number of pairs (i, j) with $i > j$ and $A_i = A_j$ is $\mathfrak{C}$.

We know that there is a unique partition of d corresponding to each pair (i,j), $i>j$ such that $A_i=A_j$. Hence by Box Principle, there exists at least $\frac{\mathfrak{C}}{2^{\omega(d)-\theta}-1}$ pairs of (i,j), $i>j$ with $A_i=A_j$ and a partition (d_1,d_2) of d corresponding to these pairs. For every such pair (i,j), we write $X_i-X_j=d_1r_{ij}$, $X_i+X_j=d_2s_{ij}$. Then $\gcd(X_i-X_j,X_i+X_j)=2$ and $24\mid(X_i^2-X_j^2)$. Let r'_{ij}, s'_{ij} be such that $r'_{ij}\mid r_{ij}$, $s'_{ij}\mid s_{ij}$, $\gcd(r'_{ij},s'_{ij})=1$ and $r_{ij}s_{ij}=\frac{24}{\rho 2^{\delta}}r'_{ij}s'_{ij}$. Then

$$r'_{ij}s'_{ij}=\frac{\rho 2^{\delta}}{24}r_{ij}s_{ij}=\frac{\rho 2^{\delta}}{24}\frac{X_i^2-X_j^2}{d}=\frac{\rho 2^{\delta}}{24}\frac{i-j}{A_i}<\frac{\rho 2^{\delta}}{24}\frac{k}{A_i}<c2^{\omega(d)-3}$$

since $A_i>\frac{\rho 2^{\delta}k}{3c2^{\omega(d)}}$. There are at most $\sum_{i=1}^{c2^{\omega(d)-3}-1}2^{\omega(i)}$ possible pairs of (r'_{ij},s'_{ij}), and hence an equal number of possible pairs of (r_{ij},s_{ij}). By Lemma 9, we estimate

$$\sum_{i=1}^{c2^{\omega(d)-3}-1}2^{\omega(i)}\le\eta(c2^{\omega(d)-3})c2^{\omega(d)-3}(\log c2^{\omega(d)-3}).$$

Thus if we have

$$\frac{\mathfrak{C}}{2^{\omega(d)-\theta}-1}>\eta(c2^{\omega(d)-3})c2^{\omega(d)-3}(\log c2^{\omega(d)-3}),$$

then there exist distinct pairs $(i,j)\neq(g,h)$, $i>j$, $g>h$ with $A_i=A_j$, $A_g=A_h$ such that $r_{ij}=r_{gh}$, $s_{ij}=s_{gh}$ giving

$$X_i-X_j=d_1r_{ij}=X_g-X_h\quad\text{and}\quad X_i+X_j=d_2s_{ij}=X_g+X_h.$$

Thus $X_i=X_g$, $X_j=X_h$ implying $(i,j)=(g,h)$, a contradiction. Hence

$$\frac{\mathfrak{C}}{2^{\omega(d)-\theta}-1}\le\eta(c2^{\omega(d)-3})c2^{\omega(d)-3}(\log c2^{\omega(d)-3}),s$$

implying (28). □

The following lemma is a refinement of [16, Lemma 2].

Lemma 11. *Let $i>j,g>h,0\le i,j,g,h<k$ be such that*

$$a_i=a_j,\quad a_g=a_h \tag{29}$$

and

$$x_i - x_j = d_1 r_1, \quad x_i + x_j = d_2 r_2, \quad x_g - x_h = d_1 s_1, \quad x_g + x_h = d_2 s_2 \tag{30}$$

where (d_1, d_2) *is a partition of* d*;* $r_1 \equiv s_1 \pmod 2$, $r_2 \equiv s_2 \pmod 2$ *when* d *is even; and either* $r_1 \equiv s_1 \pmod 2$ *and* $a_i \equiv a_g \pmod 4$ *or* $2 \mid \gcd(r_1, s_1)$ *when* d *is odd. Then we have either*

$$a_i = a_g,\ r_1 = s_1 \quad \text{or} \quad a_i = a_g,\ r_2 = s_2 \tag{31}$$

or (4) *and* (5) *hold.*

Proof. We follow the proof of [16, Lemma 2]. Suppose that (31) does not hold. Then

$$a_i r_1^2 - a_g s_1^2 \neq 0, \quad a_i r_2^2 - a_g s_2^2 \neq 0. \tag{32}$$

We proceed as in [16, Lemma 2] to conclude from $d \mid (a_i x_i^2 - a_g x_g^2)$ that

$$\begin{aligned} d_1 d_2 = d \mid \frac{1}{4}\Big\{&(a_i r_1^2 - a_g s_1^2) d_1^2 + (a_i r_2^2 - a_g s_2^2) d_2^2 \\ &+ 2d(a_i r_1 r_2 - a_g s_1 s_2)\Big\}. \end{aligned} \tag{33}$$

Thus we have

$$(a_i r_1^2 - a_g s_1^2) d_1^2 = a_i (x_i - x_j)^2 - a_g (x_g - x_h)^2 \neq 0$$

and

$$(a_i r_2^2 - a_g s_2^2) d_2^2 = a_i (x_i + x_j)^2 - a_g (x_g + x_h)^2 \neq 0.$$

Since

$$n \leq a_j x_j^2 < a_i x_i x_j < a_i x_i^2 \leq n + (k-1)d$$

and

$$n \leq a_h x_h^2 < a_g x_g x_h < a_g x_g^2 \leq n + (k-1)d,$$

we have

$$\big| a_i x_i x_j - a_g x_g x_h \big| < (k-1)d. \tag{34}$$

Also

$$|a_i x_i^2 - a_g x_g^2| = |i - g| d \leq (k-1)d \tag{35}$$

$$|a_j x_j^2 - a_h x_h^2| = |j-h|d \le (k-1)d \tag{36}$$

and

$$n \le \min\left\{\frac{1}{4}a_i(x_i+x_j)^2, \frac{1}{4}a_g(x_g+x_h)^2\right\}. \tag{37}$$

Hence we derive from (34), (35) and (37) that

$$\left|(a_i r_2^2 - a_g s_2^2)d_2^2\right| < 4(k-1)d \tag{38}$$

$$n\left|(a_i r_1^2 - a_g s_1^2)d_1^2\right| < \frac{1}{4}(k-1)^2 d^2 \tag{39}$$

and further considering the cases $\{a_i r_1^2 > a_g s_1^2, a_i r_2^2 > a_g s_2^2\}$, $\{a_i r_1^2 > a_g s_1^2, a_i r_2^2 < a_g s_2^2\}$, $\{a_i r_1^2 < a_g s_1^2, a_i r_2^2 > a_g s_2^2\}$ and $\{a_i r_1^2 < a_g s_1^2, a_i r_2^2 < a_g s_2^2\}$, we derive

$$G(i,g) = \left|a_i r_1^2 - a_g s_1^2\right|d_1^2 + \left|a_i r_2^2 - a_g s_2^2\right|d_2^2 < 4(k-1)d. \tag{40}$$

Let $d = d_1 d_2$ be odd, $\gcd(d_1, d_2) = 1$. We have either r_1, s_1 are even and hence r_1, r_2, s_1, s_2 are even, or $a_i \equiv a_g \pmod 4$ and $r_1 \equiv s_1 \pmod 2$ and hence $r_2 \equiv s_2(\pmod 2$. Then reading modulo d_1 and d_2 separately in (33), we have

$$d_1 \mid \frac{1}{4}(a_i r_2^2 - a_g s_2^2) \quad \text{and} \quad d_2 \mid \frac{1}{4}(a_i r_1^2 - a_g s_1^2). \tag{41}$$

Therefore

$$4dd_2 = 4d_1 d_2^2 \le |a_i r_2^2 - a_g s_2^2| d_2^2 \tag{42}$$

and

$$4dd_1 = 4d_1^2 d_2 \le |a_i r_1^2 - a_g s_1^2| d_1^2. \tag{43}$$

From (40), we have

$$4d(d_1+d_2) \le G(i,g) < 4(k-1)d$$

so that

$$d = d_1 d_2 \le \left(\frac{d_1+d_2}{2}\right)^2 < \frac{(k-1)^2}{4}.$$

This gives (4). Again from (43) and (39), we see that $4ndd_1 < \frac{1}{4}(k-1)^2d^2$, i.e., $n < \frac{1}{16}(k-1)^2d_2$. From (42) and (38), we have $4dd_2 < 4(k-1)d$, i.e., $d_2 < (k-1)$. Thus (5) is also valid.

Let $d = d_1d_2$ be even with $\text{ord}_2(d) = 1$ and d_1 odd. Then the x_i's are odd and therefore both r_1 and s_1 is even. We see from (33) that

$$4d_1 \bigm| (a_ir_2^2 - a_gs_2^2)d_2^2 \quad \text{and} \quad 4d_2 \bigm| (a_ir_1^2 - a_gs_1^2)d_1^2. \tag{44}$$

Since $r_1 \equiv s_1 \pmod 2$, $r_2 \equiv s_2 \pmod 2$, $\gcd(d_1, d_2) = 1$ and d_1 odd, we derive that

$$2d_1 \bigm| (a_ir_2^2 - a_gs_2^2), \quad 4d_2 \bigm| (a_ir_1^2 - a_gs_1^2).$$

Therefore

$$2dd_2 = 2d_1d_2^2 \le |a_ir_2^2 - a_gs_2^2|d_2^2, \quad 4dd_1 = 4d_1^2d_2 \le |a_ir_1^2 - a_gs_1^2|d_1^2.$$

Now we argue as above to conclude (4) and (5).

Let $d = d_1d_2$ be even with $\text{ord}_2(d) \ge 2$, $\gcd(d_1, d_2) = 2$. Then we see from (33) that (44) holds. Since $\gcd(d_1, d_2) = 2$, $r_1 \equiv s_1 \pmod 2$ and $r_2 \equiv s_2 \pmod 2$, we derive that

$$2d_1 \mid (a_ir_2^2 - a_gs_2^2), \quad 2d_2 \mid (a_ir_1^2 - a_gs_1^2).$$

Therefore

$$2dd_2 = 2d_1d_2^2 \le |a_ir_2^2 - a_gs_2^2|d_2^2, \quad 2dd_1 = 2d_1^2d_2 \le |a_ir_1^2 - a_gs_1^2|d_1^2.$$

Now we argue as above to conclude (4) and (5). □

Lemma 12. *For a prime $p < k$, let*

$$\gamma_p = \text{ord}_p\left(\prod_{a_i \in R} a_i\right), \quad \gamma_p' = 1 + \text{ord}_p((k-1)!).$$

Let $\mathfrak{m} > 1$ by any real number. Then

$$\prod_{2 \le p \le \mathfrak{m}} p^{\gamma_p - \gamma_p'} \le k^{1.5\pi(\mathfrak{m})}\left(z_1 \prod_{2<p\le\mathfrak{m}} p^{\frac{2p}{p^2-1}}\right)\left(z_2 \prod_{2<p\le\mathfrak{m}} p^{\frac{2}{p^2-1}}\right)^{-k} \tag{45}$$

where $(z_1, z_2) = (2^{\frac{4}{3}}, 2^{\frac{2}{3}})$ if d is odd and $(z_1, z_2) = (4, 2)$ if d is even.

Proof. The proof is the refinement of inequality [12, (6.4)]. Let $p^h \le k-1 < p^{h+1}$ where h is a positive integer. Then

$$\gamma'_p - 1 = \left[\frac{k-1}{p}\right] + \left[\frac{k-1}{p^2}\right] + \cdots + \left[\frac{k-1}{p^h}\right]. \tag{46}$$

Let $p \nmid d$. Then we see that g_p is the number of terms in $\{n, n+d, \ldots, n+(k-1)d\}$ divisible by p to an odd power. After removing a term to which p appears to a maximal power, the number of terms in the remaining set divisible by p to an odd power is at most

$$\left[\frac{k-1}{p}\right] - \left(\left[\frac{k-1}{p^2}\right] - 1\right) + \left[\frac{k-1}{p^3}\right] - \left(\left[\frac{k-1}{p^4}\right] - 1\right) + \ldots$$
$$+ (-1)^\epsilon \left(\left[\frac{k-1}{p^h}\right] + (-1)^\epsilon\right)$$

where $\epsilon = 1$ or 0 according as h is even or odd, respectively. We note that the above expression is always positive. Combining this with (46) and $\left[\frac{k-1}{p^i}\right] \ge \frac{k-1}{p^i} - 1 + \frac{1}{p^i} = \frac{k}{p^i} - 1$, we have

$$\begin{aligned}\gamma_p - \gamma'_p &\le -2\left\{\left[\frac{k-1}{p^2}\right] + \cdots + \left[\frac{k-1}{p^{h-1+\epsilon}}\right]\right\} + \frac{h-1+\epsilon}{2}\\ &\le -2\left\{\frac{k}{p^2} + \cdots + \frac{k}{p^{h-1+\epsilon}} - \frac{h-1+\epsilon}{2}\right\} + \frac{h-1+\epsilon}{2}\\ &= -\frac{2k}{p^2\left(1-\frac{1}{p^2}\right)}\left(1 - \frac{1}{p^{h-1+\epsilon}}\right) + 1.5(h-1+\epsilon).\end{aligned}$$

Since $p^h \ge \frac{k}{p}$ and $h < \frac{\log k}{\log p}$, we get

$$\begin{aligned}\gamma_p - \gamma'_p &< -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p} + \frac{2p^{2-\epsilon}}{p^2-1} + 1.5\epsilon - 1.5\\ &\le -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p} + \frac{2p}{p^2-1}.\end{aligned}$$

When d is even, we have $\gamma_2 - \gamma'_2 = -1 - \mathrm{ord}_2(k-1) < -k + \frac{\log k}{\log 2} + 2$ by Lemma 1 (v). Now (45) follows immediately. □

Lemma 13. *Suppose that $n \geq c_1(k-1)^3$ or $d \geq 4c_1(k-1)^2$ or both. Let $1 \leq \varrho \leq 2^{\omega(d)-\theta}$ be the greatest integer such that $R_\varrho = \{a_i \mid \nu(a_i) = \varrho\} \neq \phi$. For $k \geq \kappa_0$, we have*

$$\mathfrak{r} = \left|\{(i,j) \mid a_i = a_j,\ i > j\}\right| \geq g(\varrho) := \begin{cases} 4\varrho(2^{\omega(d)} - 1) & \text{if } d \text{ is odd,} \\ 2\varrho(2^{\omega(d)-\theta} - 1) & \text{if } d \text{ is even.} \end{cases}$$

Proof. We have

$$k = \sum_{\mu=1}^{\varrho} \mu r_\mu \quad \text{and} \quad |R| = \sum_{\mu=1}^{\varrho} r_\mu$$

where $r_\mu = |R_\mu = \{a_i \mid \nu(a_i) = \mu\}|$. Each R_μ gives rise to $\frac{\mu(\mu-1)}{2} r_\mu$ pairs of i, j with $i > j$ such that $a_i = a_j$. Then

$$\mathfrak{r} = \sum_{\mu=1}^{\varrho} \frac{\mu(\mu-1)}{2} r_\mu = k - |R| + \sum_{\mu=1}^{\varrho} \frac{(\mu-1)(\mu-2)}{2} r_\mu.$$

Suppose that the assertion of the Lemma 13 does not hold. Then $g(\varrho) > k - |R| + \sum_{\mu=1}^{\varrho} \frac{(\mu-1)(\mu-2)}{2} r_\mu$. We have

$$g(\varrho) - \sum_{\mu=1}^{\varrho} \frac{(\mu-1)(\mu-2)}{2} r_\mu \leq g(\varrho) - \frac{(\varrho-1)(\varrho-2)}{2} := g_0(\varrho).$$

We see that $g_0(\varrho)$ is an increasing function of ϱ. Since $\varrho \leq 2^{\omega(d)-\theta}$, we find that

$$k - |R| < g_0(2^{\omega(d)-\theta}) = (2^{\omega(d)-\theta} - 1)(z_3 2^{\omega(d)-\theta} + 1) := g_1$$

where $z_3 = \frac{7}{2}$ if d is odd and $\frac{3}{2}$ if d is even. Thus $|R| > k - g_1$. Since the a_i's are squarefree, we have by Lemma 8 that

$$\prod_{a_i \in R} a_i \geq z_4^{k-g_1}(k - g_1)!$$

where $z_4 = 1.6$ if d is odd and 2.4 if d is even. Also, we have

$$\prod_{a_i \in R} a_i \,\Big|\, (k-1)! \left(\prod_{p<k} p \right) \prod_{2 \leq p \leq \mathfrak{m}} p^{\gamma_p - \gamma'_p}$$

where γ_p, γ'_p and $\mathfrak{m}$ are as in Lemma 12. This with (45) and Lemma 1 (iv) gives

$$\prod_{a_i \in R} a_i < k!k^{1.5\pi(\mathfrak{m})-1}\left(z_1 \prod_{2<p\leq \mathfrak{m}} p^{\frac{2p}{p^2-1}}\right)\left(\frac{z_2}{2.7205} \prod_{2<p\leq \mathfrak{m}} p^{\frac{2}{p^2-1}}\right)^{-k}.$$

Comparing the lower and upper bounds, we have

$$\frac{z_4^{g_1}k!}{(k-g_1)!} > k^{-1.5\pi(\mathfrak{m})+1}\left(z_1 \prod_{2<p\leq \mathfrak{m}} p^{\frac{2p}{p^2-1}}\right)^{-1}\left(\frac{z_2 z_4}{2.7205} \prod_{2<p\leq \mathfrak{m}} p^{\frac{2}{p^2-1}}\right)^{k}. \quad (47)$$

By Lemma 2, we have

$$\frac{z_4^{g_1}k!}{(k-g_1)!} < z_4^{g_1}e^{-g_1}k^{g_1}\left(\frac{k}{k-g_1}\right)^{k-g_1+\frac{1}{2}} \frac{e^{\frac{1}{12k}}}{e^{\frac{1}{12(k-g_1)+1}}}.$$

Since $k \geq \kappa_0$, we find that $g_1 < \frac{k}{z_5}$ for $\omega(d) \geq 12$ where $z_5 = 37, 18$ for d odd and d even, respectively. Thus

$$\frac{z_4^{g_1}k!}{(k-g_1)!} < \begin{cases} \left(\frac{z_4(k-g_1)}{e}\right)^{g_1}\left(\frac{k}{k-g_1}\right)^{k+\frac{1}{2}} & \text{if } \omega(d) \leq 11, \\ \left(\frac{z_5}{z_5-1}\right)^{k+\frac{1}{2}}\left(\frac{(z_4(z_5-1)k}{z_5 e}\right)^{g_1} & \text{if } \omega(d) \geq 12. \end{cases}$$

Hence we derive from (47) that

$$\begin{aligned} g_1 > & \frac{k\log\left(\frac{z_2z_4}{2.7205}\prod_{2<p\leq\mathfrak{m}} p^{\frac{2}{p^2-1}}\right) + (k+\frac{1}{2})\log(1-\frac{g_1}{k})}{\log(k-g_1)-1+\log z_4} \\ & -\frac{(1.5\pi(\mathfrak{m})-1)\log k + \log\left(z_1\prod_{2<p\leq\mathfrak{m}} p^{\frac{2p}{p^2-1}}\right)}{\log(k-g_1)-1+\log z_4} \end{aligned} \quad (48)$$

for $\omega(d) \leq 11$ and

$$g_1 > \frac{k\log\left(\frac{z_5-1}{z_5}\frac{z_2z_4}{2.7205}\prod\limits_{2<p\leq\mathfrak{m}} p^{\frac{2}{p^2-1}}\right) - (1.5\pi(\mathfrak{m})-1)\log k - \log\left(\sqrt{\frac{z_5}{z_5-1}}z_1\prod\limits_{2<p\leq\mathfrak{m}} p^{\frac{2p}{p^2-1}}\right)}{\log k - 1 + \log z_4(z_5-1) - \log z_5} \quad (49)$$

for $\omega(d) \geq 12$.

Let $\omega(d) \le 11$. Taking $\mathfrak{m} = \min(1000, \sqrt{\kappa_0}\,)$ in (48), we observe that the right hand side of (48) is an increasing function of k and the inequality does not hold at $k = \kappa_0$. Hence (48) is not valid for all $k \ge \kappa_0$. For instance, when $\omega(d) = 4$, d odd, we have $\kappa_0 = 15700$ and $g_1 = 855$. With these values, we see that the right hand side of (48) exceeds 855 at $k = 15300$, a contradiction. Hence (48) is not valid for all $k \ge 15300$.

Let $\omega(d) \ge 12$. Taking $\mathfrak{m} = 1000$ in (49), we derive that

$$g_1 > \begin{cases} 0.63104\dfrac{k}{\log k} & \text{if } d \text{ is odd,} \\[2ex] 1.183\dfrac{k}{\log k} & \text{if } d \text{ is even.} \end{cases}$$

For d odd, we see that

$$0.63104\frac{k}{\log k} \ge 0.63104\frac{\kappa_0}{\log \kappa_0}$$
$$= \frac{0.63104 \times 11\omega(d)4^{\omega(d)}}{\omega(d)\log 4 + \log 11 + \log \omega(d)} > \frac{7}{2}4^{\omega(d)} > g_1,$$

a contradiction. Similarly, we get a contradiction for d even. □

Lemma 14. *Let $k \ge \kappa_0 = \kappa_0(\omega(d))$. Assume that $d < 4c_1(k-1)^2$. Let $T_1 = \{0 \le i < k \mid X_i > 1\}$ defined in Section 2 be such that*

$$|T_1| > C_1 := \begin{cases} \dfrac{k}{C_2} + \dfrac{k}{48} + C_3 + \dfrac{8}{3} & \text{if } \ \omega(d) = 2, \\[2ex] \dfrac{k}{C_2} + \dfrac{k}{12} + C_3 + \dfrac{2^{\omega(d)+1}}{3} & \text{if } \ \omega(d) = 3, 4, 5, \\[2ex] \dfrac{k}{C_2} + \dfrac{k}{12} + \dfrac{k}{9} + & \text{if } \ \omega(d) \ge 6, \end{cases}$$

where $C_2 \le 2k^{\frac{1}{3}}$ and $C_3 = 39, 42, 195, 806$ for $\omega(d) = 2, 3, 4, 5$, respectively. Then

$$\max_{i \in T_1} A_i \ge 2^{\delta} C_0 \frac{k}{C_2} \text{ where } C_0 = C_0(\omega(d)) = \begin{cases} 1 & \text{if } \omega(d) = 2, \\[2ex] \dfrac{3}{4}2^{[\frac{\omega(d)}{3}]} & \text{if } \omega(d) \ge 3. \end{cases} \quad (50)$$

Proof. We see that for $\omega(d) \geq 6$,

$$\frac{k}{20 \cdot 2^{\omega(d)}} \geq \left(4c_1(k-1)^2\right)^{\frac{1}{\omega(d)}} > d^{\frac{1}{\omega(d)}}$$

where c_1 is given by Proposition 2. Hence there exists a partition $d = d_1 d_2$ of d with

$$d_1 < \frac{k}{20 \cdot 2^{\omega(d)}} \quad \text{with} \quad \omega(d_1) \geq 1 \quad \text{and} \quad \omega(d_2) \leq \omega(d) - 1.$$

Therefore

$$\nu(A_i) \leq 2^{\omega(d_2)} \leq 2^{\omega(d)-1} \quad \text{for } A_i \geq \frac{k}{20 \cdot 2^{\omega(d)}} \tag{51}$$

by Lemma 4.

Let

$$T_2 = \left\{ i \in T_1 \mid A_i > \frac{2^\delta \rho k}{3c2^{\omega(d)}} \right\}, \quad T_3 = T_1 - T_2, \tag{52}$$

where $c = 16$ if $\omega(d) = 2$, $c = 4$ if $\omega(d) = 3, 4, 5$ and $c = 2$ if $\omega(d) \geq 6$. Further let

$$S_2 = \{A_i \mid i \in T_2\}, \quad S_3 = \{A_i \mid i \in T_3\} \tag{53}$$

and $|S_3| = s$. Then considering residue classes modulo $2^\delta \rho$, we derive that

$$\frac{2^\delta \rho k}{3c \cdot 2^{\omega(d)}} \geq \max_{A_i \in S_3} A_i \geq 2^\delta \rho (s-1) + 1$$

so that $|S_3| = s \leq \frac{k}{3c2^{\omega(d)}} - \frac{1}{\rho} + 1 \leq \frac{k}{3c2^{\omega(d)}} + \frac{2}{3}$. We see from Corollary 1, (51), (52) and (53) that

$$\begin{aligned} |T_3| &\leq \frac{k}{20 \cdot 2^{\omega(d)}} 2^{\omega(d)} + \left(\frac{k}{6 \cdot 2^{\omega(d)}} - \frac{k}{20 \cdot 2^{\omega(d)}} + \frac{2}{3} \right) 2^{\omega(d)-1} \\ &\leq \frac{k}{20} + \left(\frac{k}{6} - \frac{k}{20} \right) 2^{-1} + \frac{2}{3} 2^{\omega(d)-1} \leq \frac{k}{12} + \frac{k}{40} + \frac{k}{6 \times 2^6} \leq \frac{k}{9} \end{aligned}$$

if $\omega(d) \geq 6$ and

$$|T_3| \leq \begin{cases} \left(\frac{k}{48 \cdot 2^{\omega(d)}} + \frac{2}{3}\right) 2^{\omega(d)} = \frac{k}{48} + \frac{8}{3} & \text{if } \omega(d) = 2, \\ \left(\frac{k}{12 \cdot 2^{\omega(d)}} + \frac{2}{3}\right) 2^{\omega(d)} = \frac{k}{12} + \frac{2^{\omega(d)+1}}{3} & \text{if } \omega(d) = 3, 4, 5. \end{cases}$$

Therefore

$$|T_2| > C_1 - |T_3| \geq C_4 := \begin{cases} \frac{k}{C_2} + C_3 & \text{if } \omega(d) = 2, 3, 4, 5, \\ \frac{k}{C_2} + \frac{k}{4} & \text{if } \omega(d) \geq 6. \end{cases}$$

Let $\mathfrak{C}$, $\mathfrak{C}_\mu$ be as in Lemma 10 with $c = 16$ if $\omega(d) = 2$, $c = 4$ if $\omega(d) = 3, 4, 5$ and $c = 2$ if $\omega(d) \geq 6$. Then $C_4 < |T_2| = |S_2| + \sum_{\mu \geq 2} (\mu - 1)|\mathfrak{C}_\mu|$. Now we apply Lemma 10 and use $k \geq \kappa_0 \geq \eta(2^{\omega(d)-2})(\log 2^{\omega(d)-2}) 2^{\omega(d)} (2^{\omega(d)-\theta} - 1)$ for $\omega(d) \geq 6$ to get

$$C_4 < \begin{cases} |S_2| + C_3 & \text{if } 2 \leq \omega(d) \leq 5, \\ |S_2| + \frac{k}{12} & \text{if } \omega(d) \geq 6. \end{cases}$$

Thus

$$|S_2| > \frac{k}{C_2}.$$

Let $\omega(d) = 2$. Then considering the A_i's modulo 2^δ, we see that

$$\max_{A_i \in S_2} A_i \geq 2^\delta \left[\frac{k}{C_2}\right] + \frac{2^\delta k}{48 \times 4} \geq 2^\delta \frac{k}{C_2}$$

which gives (50). Now we take $\omega(d) \geq 3$. Since $d < 4c_1(k-1)^2$, we have $r \geq [\frac{\omega(d)}{3}]$ by Lemma 6. By (14), we have $\frac{k}{C_2} \geq \frac{k^{\frac{2}{3}}}{2} > \frac{1}{2^r}(4c_1(k-1)^2))^{\frac{1}{3}} > \prod_{j=1}^{r} \left(\frac{P_j - 1}{2}\right)$. We now apply Corollary 2 with $s = [\frac{k}{C_2} + 1]$ and $U = 1$ to get

$$\max_{A_i \in S_2} A_i \geq \frac{3}{4} 2^{r+\delta} \left[\frac{k}{C_2} + 1\right] \geq \frac{3}{4} 2^{\left[\frac{\omega(d)}{3}\right]+\delta} \frac{k}{C_2}$$

which yields (50). □

4. Proof of Proposition 2

We assume that either $n \geq c_1(k-1)^3$ or $d \geq 4c_1(k-1)^2$. Then $\nu(a_{i_0}) \leq 2^{\omega(d)-\theta}$ for $0 \leq i_0 < k$ by Lemma 5. Let ϱ be as defined in the statement of Lemma 13. Then $\nu(a_{i_0}) \leq \varrho$. By Lemma 13, there are at least $z\varrho(2^{\omega(d)}-1)$ distinct pairs (i,j) with $i > j$ and $a_i = a_j$, where $z = 4$ if d is odd and 2 if d is even. Since there can be at most $2^{\omega(d)-\theta}-1$ possible partitions of d, by Box principle, there exists a partition (d_1, d_2) of d and at least $z\varrho$ pairs of (i,j) with $a_i = a_j$, $i > j$ corresponding to this partition. We write

$$x_i - x_j = d_1 r_1(i,j) \quad \text{and} \quad x_i + x_j = d_2 r_2(i,j).$$

Let d be odd. Suppose there are at least ϱ distinct pairs $(i_1, j_1), \ldots, (i_\varrho, j_\varrho), \ldots$ with the corresponding $r_1(i,j)$ even. Then $|\{i_1, \ldots, i_\varrho, j_1, \ldots, j_\varrho\}| > \varrho$. Hence we can find $1 \leq l, m \leq \varrho$ with $(i_l, j_l) \neq (i_m, j_m)$, $a_{i_l} = a_{j_l}$, $a_{i_m} = a_{i_m}$ and $a_{i_l} \neq a_{i_m}$. Now the result follows by Lemma 11. Thus we may assume that there are at most $\varrho - 1$ pairs (i,j) with $r_1(i,j)$ even. Then there are at least $3\varrho + 1$ distinct pairs (i,j) with $r_1(i,j)$ odd. Since $a_i \equiv 1, 2, 3 \pmod 4$, we can find at least ϱ pairs with $a_i \equiv a_g \pmod 4$ for any two such pairs (i,j), (g,h). Then there exist two distinct pairs (i,j), (g,h) with $a_i = a_j$, $a_g = a_h$ and $a_i \neq a_g$ from these pairs. Also $r_1(i,j) \equiv r_1(g,h) \pmod 2$. This gives (4) and (5) by Lemma 11 which is a contradiction.

Let d be even. We observe that $8 \mid (x_i^2 - x_j^2)$ and $\gcd(x_i - x_j, x_i + x_j) = 2$. We claim that there are at least ϱ pairs with $r_1(i,j) \equiv r_1(g,h) \pmod 2$ and $r_2(i,j) \equiv r_2(g,h) \pmod 2$ for any two such distinct pairs (i,j) and (g,h). If the claim is true, then there are two pairs $(i,j) \neq (g,h)$ with $i > j$, $g > h, a_i = a_j$, $a_g = a_h$ and $a_i \neq a_g$ since $\nu(a_i) \leq \varrho$. This implies (4) and (5) by Lemma 11, contradicting our assumption. Let $\mathrm{ord}_2(d) = 1$. Then d_1 is odd, implying that $r_1(i,j)$ is even. We can choose at least ϱ pairs whose r_2's are of the same parity. Thus the claim is true in this case. Let $\mathrm{ord}_2(d) \geq 3$. Then we have either $\mathrm{ord}_2(d_1) = 1$ implying that all the r_1's are odd, or $\mathrm{ord}_2(d_2) = 1$ implying that all the r_2's are odd. Thus the claim follows. Finally, let $\mathrm{ord}_2(d) = 2$. Then $2 \parallel d_1$ and $2 \parallel d_2$ so that r_1 and r_2 are of the opposite parity for any pair and hence the claim holds. $\square$

5. Proof of Proposition 3

In this section, we assume that $k \geq \kappa_0 = \kappa_0(\omega(d))$. In view of Proposition 2, we may assume that $d < 4c_1(k-1)^2$. We may also assume that X_i is a prime for each $i \in T_1$ in the proof of Proposition 3. Otherwise $n + (k-1)d \geq (k+1)^4$, which implies the assertion.

Since $d < 4c_1(k-1)^2$, d has at least one prime divisor $\leq k$ otherwise $d > k^{\omega(d)} \geq k^2$, giving a contradiction. Thus $\pi_d(k) \leq \pi(k) - 1$. Let $n + (k-1)d \geq L$ for some $L > 0$. By Lemma 3 and Lemma 1 (i), we have

$$|T_1| > k - \frac{(k-1)\log(k-1)}{\log L - \log 2} - \frac{k}{\log k}\left(1 + \frac{1.5}{\log k}\right). \tag{54}$$

We see from [5] that $n(n+d)\dots(n+(k-1)d)$ is divisible by at least $\pi(2k) - \pi_d(k) \geq \pi(2k) - \pi(k) + 1$ primes exceeding k. Hence we have $n + (k-1)d \geq 4k^2$. Thus by taking $L = 4k^2$ in (54), we get

$$|T_1| > k - \frac{(k-1)\log(k-1)}{\log(2k^2)} - \frac{k}{\log k}\left(1 + \frac{1.5}{\log k}\right).$$

The right hand side of the above inequality is an increasing function of k and

$$|T_1| > \begin{cases} \dfrac{k}{5} + \dfrac{k}{48} + C_3 + \dfrac{8}{3} & \text{if } \omega(d) = 2, \\[2ex] \dfrac{k}{6} + \dfrac{k}{12} + C_3 + \dfrac{16}{3} & \text{if } \omega(d) = 3, \\[2ex] \dfrac{5}{24}k + \dfrac{k}{12} + C_3 + \dfrac{2^{\omega(d)+1}}{3} & \text{if } \omega(d) = 4, 5, \\[2ex] \dfrac{5}{48}k + \dfrac{k}{12} + \dfrac{k}{9} & \text{if } \omega(d) \geq 6. \end{cases} \tag{55}$$

Now we see from Lemma 14 that (50) holds with

$$C_2 = \begin{cases} 5 & \text{if } \omega(d) = 2, \\[1ex] 6 & \text{if } \omega(d) = 3, \\[1ex] \dfrac{24}{5} & \text{if } \omega(d) = 4, 5, \\[2ex] \dfrac{48}{5} & \text{if } \omega(d) \geq 6. \end{cases}$$

This gives $n+(k-1)d \geq \frac{C_0}{C_2}k^3$. Hence (7) is valid for $\omega(d) \geq 4$. Now we take $\omega(d) = 2, 3$. Putting $L = \frac{C_0}{5}k^3$ in (54), we derive that

$$|T_1| > \begin{cases} \dfrac{5k}{16} + \dfrac{k}{48} + C_3 + \dfrac{2^{\omega(d)+1}}{3} & \text{if } \omega(d) = 2, \\ \dfrac{5k}{24} + \dfrac{k}{12} + C_3 + \dfrac{2^{\omega(d)+1}}{3} & \text{if } \omega(d) = 3. \end{cases}$$

We apply Lemma 14 again to get $\max_{i \in T_1} A_i \geq 2^{\delta}\frac{5}{16}k$ so that $n+(k-1)d \geq 2^{\delta}\frac{5}{16}k^3$, which implies (7). This completes the proof. □

References

[1] B. Brindza, L. Hajdu and I. Z. Ruzsa, On the equation $x(x+d)\dots(x+(k-1)d) = by^2$, *Glasgow. Math. J.* (2000), 255–261.

[2] P. Dusart, Autour de la fonction qui compte le nombre de nombres premiers, Ph.D. thesis, *Université de Limoges*, 1998.

[3] P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 92–301.

[4] K. Győry, Power values of products of consecutive integers and binomial coefficients, Number Theory and its Applications, *Kluwer Acad. Publ.*, 1999, 145–156.

[5] S. Laishram and T. N. Shorey, Number of prime divisors in a product of terms of an arithmetic progression, *Indag Math.* **15**(4) (2004), (in press).

[6] S. Laishram, Topics in Diophantine Equations, *M.Sc. Thesis, University of Mumbai*, 2004.

[7] R. Marszalek, On the product of consecutive elements of an arithmetic progression, *Monatsh. für Math.* **100** (1985), 215–222.

[8] A. Mukhopadhyay and T. N. Shorey, Almost squares in arithmetic progression (II), *Acta Arith.* **110** (2003), 1–14.

[9] H. Robbins, A remark on Stirling's formula, *Amer. Math. Monthly* **62** (1955), 26–29.

[10] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois Jour. Math.* **6** (1962), 64–94.

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

[12] N. Saradha and T. N. Shorey, Almost squares in arithmetic progression, *Compositio Math.* **138** (2003), 73–111.

[13] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, II, *Math. Comp.* **30** (1976), 337–360.

[14] T. N. Shorey, Exponential diophantine equations involving products of consecutive integers and related equations, Number Theory, (R. P. Bambah, V. C. Dumir and R. J. Hans-Gill, eds.), *Hindustan Book Agency*, 1999, 463–495.

[15] T. N. Shorey, Powers in arithmetic progression, A Panorama in Number Theory or The View from Baker's Garden, (G. Wüstholz, ed.), *Cambridge University Press*, 2002, 325–336.

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

SHANTA LAISHRAM
SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD, MUMBAI 400005
INDIA

E-mail: shanta@math.tifr.res.in

(Received July 5, 2004; revised January 8, 2005)