ACTA ARITHMETICA
129.3 (2007)

The equation $n(n+d)\cdots(n+(k-1)d) = by^2$ with $\omega(d) \le 6$ or $d \le 10^{10}$

by

SHANTA LAISHRAM and T. N. SHOREY (Mumbai)

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 $\omega(1) = 0$. The letter p always denotes a prime number and p_i the ith prime number. Let n, d, k, b, y be positive integers such that b is squarefree, $k \ge 2$, $P(b) \le k$ and $\gcd(n,d) = 1$. We consider the equation

$$n(n+d)\cdots(n+(k-1)d) = by^2 \quad \text{in } n,d,k,b,y. \tag{1.1}$$

If $d = 1$, then (1.1) has been completely solved for $P(b) < k$ by Erdős and Selfridge [ErSe75] and for $P(b) = k$ by Saradha [Sar97]. Therefore we always suppose that $d > 1$. We observe that (1.1) has infinitely many solutions if $k = 2, 3$ and $b = 1$. Also, (1.1) with $k = 4$ implies that $b = 6$. Therefore we always suppose that $k \ge 5$ if we consider (1.1) and $k \ge 4$ if we consider (1.1) with $b = 1$. It has been conjectured that (1.1) with $k \ge 5$ does not hold. A weaker version due to Erdős states that (1.1) implies that k is bounded by an absolute constant. This has been confirmed by Marszałek [Mar85] when d is fixed and by Shorey and Tijdeman [ShTi90] when $\omega(d)$ is fixed. In fact, Shorey and Tijdeman [ShTi90] proved that (1.1) implies

$$2^{\omega(d)} > c_1 \frac{k}{\log k}, \tag{1.2}$$

which gives

$$d > k^{c_2 \log\log k}$$

where $c_1 > 0$ and $c_2 > 0$ are absolute constants. Laishram [Lai06] gave an

2000 *Mathematics Subject Classification*: Primary 11D61.
Key words and phrases: Diophantine equations, arithmetic progressions, squares, Legendre symbol, squarefree integers, congruences.

explicit version of (1.2) by showing

$$k < 11\omega(d)4^{\omega(d)} \quad \text{if } \omega(d) \geq 12 \tag{1.3}$$

and we improve this to

$$k < 2\omega(d)2^{\omega(d)}; \tag{1.4}$$

see Corollary 8.7 when $\omega(d) \geq 5$ and Theorem 3 when $\omega(d) < 5$ for a precise formulation. Equation (1.1) has been completely solved in Saradha and Shorey [SaSh03a] for $d \leq 104$ and $k \geq 4$. We prove

THEOREM 1. *Equation* (1.1) *with* $k \geq 6$ *implies that*

$$d > \max(10^{10}, k^{\log\log k}).$$

For a given value of d, we observe that (1.1) with $k \in \{4, 5\}$ can be solved via finding all the integral points on elliptic curves by MAGMA or SIMATH as in [FiHa01] and [SaSh03a]. Analogous results on higher powers for (1.1) with $k \geq 4$ and y^2 replaced by y^ℓ where $\ell > 2$ is prime are proved in Saradha and Shorey [SaSh05]; they showed that $d > 30, 5 \cdot 10^4, 10^8$ and 10^{15} according as $\ell = 3,\ 5,\ 7$ and ≥ 11, respectively. For Theorem 1, we prove several results on (1.1) which are of independent interest. For example, we solve (1.1) when $\omega(d) \leq 5,\ b = 1$ or $\omega(d) \leq 4$. We prove

THEOREM 2. *Equation* (1.1) *with* $b = 1$ *and* $\omega(d) \leq 5$ *does not hold.*

Theorem 2 contains the case $\omega(d) = 1$ already proved by Saradha and Shorey [SaSh03a]. In fact, they proved it without the assumption $\gcd(n, d) = 1$. We show that this is also not required when $\omega(d) = 2$ and $k \geq 8$ (see Section 12). We derive Theorem 2 from a more general result and we turn to introducing some notation for it.

From (1.1), we have

$$n + id = a_i x_i^2 \quad \text{for } 0 \leq i < k \tag{1.5}$$

where a_i's are squarefree such that $P(a_i) \leq \max(P(b), k-1) \leq k$. Thus (1.1) with b as the squarefree part of $a_0 a_1 \cdots a_{k-1}$ is determined by the k-tuple $(a_0, a_1, \ldots, a_{k-1})$. We rewrite (1.1) as

$$N(N-d)\cdots(N-(k-1)d) = by^2, \quad N = n + (k-1)d. \tag{1.6}$$

We call (1.6) the *mirror image* of (1.1). It is completely determined by $(a_{k-1}, \ldots, a_0)$, which we call the mirror image of $(a_0, \ldots, a_{k-1})$. Let $\mathfrak{S}_1$ be the set of tuples $(a_0, \ldots, a_{k-1})$ given by

$$\begin{aligned}
k = 8:&\ \ (2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10);\\
k = 9:&\ \ (2,3,1,5,6,7,2,1,10);\\
k = 13:&\ \ (3,1,5,6,7,2,1,10,11,3,13,14,15),\\
&\ \ (1,5,6,7,2,1,10,11,3,13,14,15,1)
\end{aligned}$$

and their mirror images. Further, let $\mathfrak{S}_2$ be the set of tuples $(a_0, a_1, \ldots, a_{k-1})$ given by

$$\begin{aligned}
k = 14 &: (3,1,5,6,7,2,1,10,11,3,13,14,15,1);\\
k = 19 &: (1,5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22);\\
k = 23 &: (5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3),\\
&\quad (6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3,7);\\
k = 24 &: (5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3,7)
\end{aligned}$$

and their mirror images.

Equation (1.1) with $k = 6$ is not possible by Bennett, Bruin, Győry and Hajdu [BBGH06]. Also, (1.1) with $k \in \{5, 7\}$ and $P(b) < k$ does not hold by Mukhopadhyay and Shorey [MuSh03] for $k = 5$ and Hirata-Kohno, Laishram, Shorey and Tijdeman [HLST07] for $k = 7$. We do not have any contribution for the cases $k \in \{5, 7\}$ and $P(b) = k$ in the next result where we solve all the equations (1.1) other than the ones given by $\mathfrak{S}_1 \cup \mathfrak{S}_2$ whenever $\omega(d) \le 4$ and therefore we assume $k \ge 8$ in Theorem 3(a). More precisely, we prove

Theorem 3.

(a) *Equation* (1.1) *with* $k \ge 8$ *and* $\omega(d) \le 4$ *implies that either* $\omega(d) = 2$, $k = 8$, $(a_0, a_1, \ldots, a_7) \in \{(3,1,5,6,7,2,1,10), (10,1,2,7,6,5,1,3)\}$ *or* $\omega(d) = 3$, $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}_1$ *or* $\omega(d) = 4$, $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}_1 \cup \mathfrak{S}_2$.

(b) *Equation* (1.1) *with* $\omega(d) \in \{5, 6\}$ *and* d *even does not hold.*

Theorem 3 contains the already proved case $\omega(d) = 1$, where it has been shown in [SaSh03a] for $k > 29$ and [MuSh03] for $4 \le k \le 29$ that (1.1) implies that either $k = 4, (n, d, b, y) = (75, 23, 6, 140)$ or $k = 5, P(b) = k$. The next result shows that it suffices to prove our Theorems 1 and 3 for $k \ge 101$ unless (1.1) is given by $\mathfrak{S}$ which is the union of $\mathfrak{S}_1, \mathfrak{S}_2$ and the set of tuples given by $k = 7, (a_0, a_1, \ldots, a_{k-1}) \in \{(2,3,1,5,6,7,2), (3,1,5,6,7,2,1), (1,5,6,7,2,1,10)\}$ and their mirror images.

Theorem $\mathcal{A}$.

(a) *Equation* (1.1) *with* $7 \le k \le 100$ *is not possible unless* $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}$.

(b) *Equation* (1.1) *with* $4 \le k \le 109$ *and* $b = 1$ *does not hold.*

This is due to Hirata-Kohno, Laishram, Shorey and Tijdeman [HLST07]. For a survey of related results, see [Sho02].

2. Notations and preliminaries. Let $k \ge 4$ and $\gamma_1 < \cdots < \gamma_t$ be integers with $0 \le \gamma_i < k$ for $1 \le i \le t$. We consider a more general equation

$$(n+\gamma_1 d)\cdots(n+\gamma_t d) = by^2 \tag{2.1}$$

in positive integers n, d, k, b, y, t with b squarefree, $P(b) \le k$ and $\gcd(n,d) = 1$. If $t = k$, we observe that $\gamma_i = i-1$ and (2.1) coincides with (1.1). It is of interest to consider the more general equation (2.1) because of possible applications. Assume that (2.1) holds. Then we have

$$n+\gamma_i d = a_{\gamma_i} x_{\gamma_i}^2 \quad \text{for } 1 \le i \le t \tag{2.2}$$

with a_{γ_i} squarefree such that $P(a_{\gamma_i}) \le k$. Also,

$$n+\gamma_i d = A_{\gamma_i} X_{\gamma_i}^2 \quad \text{for } 1 \le i \le t, \tag{2.3}$$

$P(A_{\gamma_i}) \le k$ and $\gcd(X_{\gamma_i}, \prod_{p\le k} p) = 1$. Further, we write

$$b_i = a_{\gamma_i}, \quad B_i = A_{\gamma_i}, \quad y_i = x_{\gamma_i}, \quad Y_i = X_{\gamma_i}.$$

Since $\gcd(n,d) = 1$, we see from (2.2) and (2.3) that

$$(b_i,d) = (B_i,d) = (y_i,d) = (Y_i,d) = 1 \quad \text{for } 1 \le i \le t. \tag{2.4}$$

Let

$$R = \{b_i : 1 \le i \le t\}.$$

For $b_i \in R$, let $\nu(b_i) = |\{j : 1 \le j \le t,\, b_j = b_i\}|$ and

$$\nu_{\mathrm{o}}(b_i) = |\{j : 1 \le j \le t,\, b_j = b_i,\, 2 \nmid y_j\}|,$$
$$\nu_{\mathrm{e}}(b_i) = |\{j : 1 \le j \le t,\, b_j = b_i,\, 2 \mid y_j\}|.$$

We define

$$R_\mu = \{b_i \in R : \nu(b_i) = \mu\}, \quad r_\mu = |R_\mu|, \quad \mathfrak{r} = |\{(i,j) : b_i = b_j, i > j\}|.$$

Let

$$T = \{1 \le i \le t : Y_i = 1\}, \quad T_1 = \{1 \le i \le t : Y_i > 1\}, \quad S_1 = \{B_i : i \in T_1\}.$$

Note that $Y_i > k$ for $i \in T_1$. For $i \in T_1$, we set $\nu(B_i) = |\{j \in T_1 : B_j = B_i\}|$.

Let

$$\delta = \min(3, \mathrm{ord}_2(d)), \quad \delta' = \min(1, \mathrm{ord}_2(d)) \tag{2.5}$$

and

$$\eta = \begin{cases} 1 & \text{if } \mathrm{ord}_2(d) \le 1, \\ 2 & \text{if } \mathrm{ord}_2(d) \ge 2, \end{cases} \tag{2.6}$$

$$\varrho = \begin{cases} 3 & \text{if } 3 \mid d, \\ 1 & \text{if } 3 \nmid d. \end{cases} \tag{2.7}$$

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

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

and we always suppose that d_1 is odd if $\mathrm{ord}_2(d'') = 1$. We call such pairs (d_1, d_2) *partitions* of d''. We observe that the number of partitions of d'' is $2^{\omega(d'')-\theta_1}$ where

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

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

Let $b_i = b_j, i > j$. Then from (2.2) and (2.4), we have

$$\frac{\gamma_i - \gamma_j}{b_i} d' = \frac{y_i^2 - y_j^2}{d''} = \frac{(y_i - y_j)(y_i + y_j)}{d''}, \tag{2.8}$$

so that $\gcd(d'', y_i - y_j, y_i + y_j)$ is 1 if d'' is odd and 2 if d'' is even. Thus a pair (i, j) with $i > j$ and $b_i = b_j$ corresponds to a partition (d_1, d_2) of d'' such that $d_1 \mid (y_i - y_j)$, $d_2 \mid (y_i + y_j)$ and it is unique. Similarly, we have a unique partition of d'' corresponding to every pair (i, j) whenever $B_i = B_j$, $i, j \in T_1$.

Let $\mathfrak{p}_1 < \mathfrak{p}_2 < \cdots$ be the odd primes dividing d. Let

$$d = \begin{cases} 2^\delta \mathfrak{q}_1 \cdots \mathfrak{q}_{\omega(d)-1} & \text{if } \delta = 1, 2, \\ \mathfrak{q}_1 \cdots \mathfrak{q}_{\omega(d)} & \text{otherwise,} \end{cases}$$

where $\mathfrak{q}_1 < \cdots < \mathfrak{q}_{\omega(d)-\theta}$ are prime powers dividing $d/2^{\delta\theta}$. By induction, we have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_h \le \mathfrak{q}_1 \cdots \mathfrak{q}_h \le \left(\frac{d}{2^{\delta\theta}}\right)^{h/(\omega(d)-\theta)} \tag{2.9}$$

for any h with $1 \le h \le \omega(d) - \theta$. Further, we define

$$\mathcal{A}_h = \{B_i \in T_1 : B_i < \mathfrak{q}_1 \cdots \mathfrak{q}_h\}, \qquad \lambda_h = |\mathcal{A}_h| \tag{2.10}$$

for any h with $1 \le h \le \omega(d) - \theta$.

3. Upper bound for $n + (k-1)d$. In this section, we assume that (2.1) holds. Let $i > j$, $g > h$, $0 \le i, j, g, h < k$ be such that

$$b_i = b_j, \qquad b_g = b_h, \qquad \gamma_i + \gamma_j \ge \gamma_g + \gamma_h, \tag{3.1}$$

$$y_i - y_j = d_1 r_1, \quad y_i + y_j = d_2 r_2, \quad y_g - y_h = d_1 s_1, \quad y_g + y_h = d_2 s_2 \tag{3.2}$$

where (d_1, d_2) is a partition of d. We write $V(i, j, g, h, d_1, d_2)$ for such double pairs. We call $V(i, j, g, h, d_1, d_2)$ *degenerate* if

$$b_i = b_g,\ r_1 = s_1 \quad \text{or} \quad b_i = b_g,\ r_2 = s_2. \tag{3.3}$$

Otherwise we call it *non-degenerate*. Let q_1 and q_2 be given by

$$|b_i r_1^2 - b_g s_1^2| = q_1 d_2 \quad \text{and} \quad |b_i r_2^2 - b_g s_2^2| = q_2 d_1. \tag{3.4}$$

We shall also write $V(i, j, g, h, d_1, d_2) = V(i, j, g, h, d_1, d_2, q_1, q_2)$.

Let Ω be a set of pairs (i,j) with $i>j$ such that $b_i=b_j$. Then we say that Ω has *Property ND* if the following holds: For any two distinct pairs (i,j) and (g,h) in Ω corresponding to a partition (d_1,d_2) of d, the double pair $V(i,j,g,h,d_1,d_2)$ is non-degenerate.

In this section, we give an upper bound for $n+(k-1)d$ whenever it is possible to find a non-degenerate double pair. The next section gives a lower bound for $n+(k-1)d$. As in [ShTi90], the proofs of our theorems depend on showing that the upper bound and lower bound for $n+(k-1)d$ are not consistent whenever it is possible to find a non-degenerate double pair. Further, we show in this section that this is always the case whenever $k-|R|\geq 2^{\omega(d)-\theta}$. If we do not have this, we use Lemmas 5.4 and 7.6 depending on an idea of Erdős to give an upper bound for k. Thus there are only finitely many possibilities for k and we use counting arguments given in Section 6 to exclude these possibilities. For example, we show in Lemma 7.5 that k is large whenever d is divisible by two small primes. This is very useful in our proofs and increases considerably the lower bound for d in Theorem 1. The computations in this paper were carried out using MATHEMATICA.

We begin with the following result.

LEMMA 3.1. *Let $d=\theta_1(k-1)^2$, $n=\theta_2(k-1)^3$ with $\theta_1>0$ and $\theta_2>0$. Let $V(i,j,g,h,d_1,d_2,q_1,q_2)$ be a non-degenerate double pair. Then*

$$\theta_2<\frac{1}{2}\left\{\frac{1}{q_1q_2}-\theta_1+\sqrt{\frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}}\right\} \tag{3.5}$$

and

$$d_1<\frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)},\qquad d_2<\frac{4(k-1)}{q_2}. \tag{3.6}$$

Proof. From (3.2) we have $y_i=(d_1r_1+d_2r_2)/2$ and $y_g=(d_1s_1+d_2s_2)/2$. Further, from (2.2) and (3.1), we get

$$\begin{aligned}(\gamma_i-\gamma_g)d&=b_iy_i^2-b_gy_g^2\\ &=\tfrac{1}{4}\{(b_ir_1^2-b_gs_1^2)d_1^2+(b_ir_2^2-b_gs_2^2)d_2^2+2d(b_ir_1r_2-b_gs_1s_2)\}.\end{aligned}$$

We observe from (3.2), (3.1) and (2.2) that $b_ir_1r_2=\gamma_i-\gamma_j$, $b_gs_1s_2=\gamma_g-\gamma_h$. Therefore

$$2(\gamma_i+\gamma_j-\gamma_g-\gamma_h)d=(b_ir_1^2-b_gs_1^2)d_1^2+(b_ir_2^2-b_gs_2^2)d_2^2. \tag{3.7}$$

Then reading modulo d_1,d_2 separately in (3.7), we have

$$\begin{aligned}&d_2\,|\,(b_ir_1^2-b_gs_1^2),\quad d_1\,|\,(b_ir_2^2-b_gs_2^2)\quad\text{if }\operatorname{ord}_2(d)\leq 1,\\ &\frac{d_2}{2}\,|\,(b_ir_1^2-b_gs_1^2),\quad \frac{d_1}{2}\,|\,(b_ir_2^2-b_gs_2^2)\quad\text{if }\operatorname{ord}_2(d)\geq 2.\end{aligned} \tag{3.8}$$

Hence $2q_1, 2q_2$ are non-negative integers. We see that $q_1 \neq 0$ and $q_2 \neq 0$ since $V(i,j,g,h,d_1,d_2,q_1,q_2)$ is non-degenerate. Further, we see from (2.2) that

$$b_iy_i^2 - b_gy_g^2 = (\gamma_i - \gamma_g)d, \quad b_jy_j^2 - b_hy_h^2 = (\gamma_j - \gamma_h)d. \tag{3.9}$$

Therefore, by (3.2), we have

$$\begin{aligned} 0 \neq F_1 &:= (b_ir_1^2 - b_gs_1^2)d_1^2 = b_i(y_i - y_j)^2 - b_g(y_g - y_h)^2 \\ &= (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d - 2(b_iy_iy_j - b_gy_gy_h), \end{aligned} \tag{3.10}$$

$$\begin{aligned} 0 \neq F_2 &:= (b_ir_2^2 - b_gs_2^2)d_2^2 = b_i(y_i + y_j)^2 - b_g(y_g + y_h)^2 \\ &= (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d + 2(b_iy_iy_j - b_gy_gy_h). \end{aligned} \tag{3.11}$$

We note here that $F_1 < 0, F_2 < 0$ is not possible since $\gamma_i + \gamma_j \geq \gamma_g + \gamma_h$.

Let a and b be positive real numbers with $a \neq b$. We have

$$2\sqrt{ab} = (a+b)\left(1 - \left(\frac{a-b}{a+b}\right)^2\right)^{1/2}.$$

By using $1 - x < (1-x)^{1/2} < 1 - x/2$ for $0 < x < 1$, we get

$$a + b - \frac{(a-b)^2}{a+b} < 2\sqrt{ab} < a + b - \frac{(a-b)^2}{2(a+b)}.$$

We use it with $a = n + \gamma_i d$ and $b = n + \gamma_j d$ so that $\sqrt{ab} = b_iy_iy_j$ by (2.2) and (3.1). We obtain

$$\begin{aligned} &2n + (\gamma_i + \gamma_j)d - \frac{(\gamma_i - \gamma_j)^2d^2}{2n + (\gamma_i + \gamma_j)d} \\ &\qquad < 2b_iy_iy_j < 2n + (\gamma_i + \gamma_j)d - \frac{(\gamma_i - \gamma_j)^2d^2}{4n + 2(\gamma_i + \gamma_j)d}. \end{aligned} \tag{3.12}$$

Similarly, we get

$$\begin{aligned} &2n + (\gamma_g + \gamma_h)d - \frac{(\gamma_g - \gamma_h)^2d^2}{2n + (\gamma_g + \gamma_h)d} \\ &\qquad < 2b_gy_gy_h < 2n + (\gamma_g + \gamma_h)d - \frac{(\gamma_g - \gamma_h)^2d^2}{4n + 2(\gamma_g + \gamma_h)d}. \end{aligned} \tag{3.13}$$

Therefore (3.4), (3.10), (3.12) and (3.13) yield

$$\begin{aligned} q_1dd_1 < (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d - (2n + (\gamma_i + \gamma_j)d) + \frac{(\gamma_i - \gamma_j)^2d^2}{2n + (\gamma_i + \gamma_j)d} \\ + (2n + (\gamma_g + \gamma_h)d) - \frac{(\gamma_g - \gamma_h)^2d^2}{4n + 2(\gamma_g + \gamma_h)d} \quad \text{if } F_1 > 0 \end{aligned}$$

and

$$q_1dd_1 < (2n+(\gamma_i+\gamma_j)d) - \frac{(\gamma_i-\gamma_j)^2d^2}{4n+2(\gamma_i+\gamma_j)d} - (2n+(\gamma_g+\gamma_h)d) + \frac{(\gamma_g-\gamma_h)^2d^2}{2n+(\gamma_g+\gamma_h)d} - (\gamma_i+\gamma_j-\gamma_g-\gamma_h)d \quad \text{if } F_1<0.$$

Thus

$$(3.14)\quad q_1d_1 < \begin{cases} \dfrac{(\gamma_i-\gamma_j)^2d}{2n+(\gamma_i+\gamma_j)d} = \dfrac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)} & \text{if } F_1>0,\\ \dfrac{(\gamma_g-\gamma_h)^2d}{2n+(\gamma_g+\gamma_h)d} = \dfrac{\theta_1(\gamma_g-\gamma_h)^2}{2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h)} & \text{if } F_1<0.\end{cases}$$

Similarly from (3.4), (3.11), (3.12) and (3.13), we have

$$(3.15)\quad q_2d_2 < \begin{cases} 2(\gamma_i+\gamma_j-\gamma_g-\gamma_h) + \dfrac{\theta_1(\gamma_g-\gamma_h)^2}{2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h)} & \text{if } F_2>0,\\ \dfrac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)} - 2(\gamma_i+\gamma_j-\gamma_g-\gamma_h) & \text{if } F_2<0.\end{cases}$$

Let

$$n_{i,j} := (k-1)^2\left\{\theta_2(k-1)+\frac{\theta_1(\gamma_i+\gamma_j)}{2} - \frac{\theta_1^2(\gamma_i-\gamma_j)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))}\right\},$$

$$n_{g,h} := (k-1)^2\left\{\theta_2(k-1)+\frac{\theta_1(\gamma_g+\gamma_h)}{2} - \frac{\theta_1^2(\gamma_g-\gamma_h)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h))}\right\}.$$

Then we see from (3.12) and (3.13) that $n_{i,j} < b_iy_iy_j < \frac{1}{4}b_i(y_i+y_j)^2$ and $n_{g,h} < b_gy_gy_h < \frac{1}{4}b_g(y_g+y_h)^2$. Assume $F_1>0$. Then from (3.4), (3.11) and (3.2), we have

$$n_{i,j}q_1d_2d_1^2 < \tfrac{1}{4}b_i(y_i+y_j)^2b_i(y_i-y_j)^2 = \tfrac{1}{4}(\gamma_i-\gamma_j)^2d^2,$$

which implies

$$(3.16)\quad \theta_1+\theta_2 = \frac{n_{i,j}}{(k-1)^3} + \frac{\theta_1}{k-1}\left(k-1-\frac{\gamma_i+\gamma_j}{2}+\frac{\theta_1(\gamma_i-\gamma_j)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))}\right) < \frac{(\gamma_i-\gamma_j)^2}{4q_1(k-1)^3}\,d_2+\theta_1 \le \frac{d_2}{4q_1(k-1)}+\theta_1 \quad \text{if } F_1>0$$

by estimating

$$\frac{\theta_1(\gamma_i-\gamma_j)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))} \le \frac{(\gamma_i-\gamma_j)^2}{2(\gamma_i+\gamma_j)} < \frac{\gamma_i+\gamma_j}{2}.$$

Similarly

$$\theta_1+\theta_2<\frac{d_2}{4q_1(k-1)}+\theta_1 \quad \text{if } F_1<0. \tag{3.17}$$

We separate the possible cases:

CASE I: $F_1>0,\ F_2>0$. From (3.14) and (3.15), we have

$$\begin{aligned}
&q_1q_2\theta_1(k-1)^2\\
&<\frac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)}\left\{2(\gamma_i+\gamma_j-\gamma_g-\gamma_h)+\frac{\theta_1(\gamma_g-\gamma_h)^2}{2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h)}\right\}\\
&<\frac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)}\{2(\gamma_i+\gamma_j)-2(\gamma_g+\gamma_h)+\gamma_g-\gamma_h\}\\
&<\frac{2\theta_1(\gamma_i-\gamma_j)^2(\gamma_i+\gamma_j)}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)}\le\frac{2\theta_1\gamma_i^3}{2\theta_2(k-1)+\theta_1\gamma_i}\le\frac{2\theta_1(k-1)^3}{2\theta_2(k-1)+\theta_1(k-1)}
\end{aligned}$$

since $2\theta_1\gamma_i^3/(2\theta_2(k-1)+\theta_1\gamma_i^3)$ is an increasing function of γ_i. Therefore $2\theta_2+\theta_1<2/q_1q_2$, which gives (3.5). Further, from (3.14) and (3.15), we have

$$\begin{aligned}
d_1&<\frac{\theta_1(\gamma_i-\gamma_j)^2}{q_1(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))}<\frac{\theta_1\gamma_i^2}{q_1(2\theta_2(k-1)+\theta_1\gamma_i)}\le\frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)},\\
d_2&<\frac{1}{q_2}\{2(\gamma_i+\gamma_j)-2(\gamma_g+\gamma_h)+\gamma_g-\gamma_h\}<\frac{2(\gamma_i+\gamma_j)}{q_2}<\frac{4(k-1)}{q_2},
\end{aligned}$$

hence (3.6).

CASE II: $F_1>0,\ F_2<0$. From (3.14), we have

$$d_1<\frac{\theta_1(\gamma_i-\gamma_j)^2}{q_1(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))}<\frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)}.$$

Similarly

$$d_2<\frac{1}{q_2}\,\frac{\theta_1(k-1)}{2\theta_2+\theta_1}<\frac{k-1}{q_2}$$

from (3.15) and $\gamma_i+\gamma_j\ge\gamma_g+\gamma_h$. Therefore (3.6) follows. Further,

$$\theta_1(k-1)^2=d=d_1d_2<\frac{\theta_1^2(k-1)^2}{q_1q_2(2\theta_2+\theta_1)^2}$$

implying $(2\theta_2+\theta_1)^2<\theta_1/q_1q_2$. Hence (3.5) follows.

CASE III: $F_1<0,\ F_2>0$. From (3.14) and (3.15), we have

$$\theta_1(k-1)^2<\frac{\theta_1\gamma_g^2}{q_1q_2(2\theta_2(k-1)+\theta_1\gamma_g)}\left\{2(\gamma_i+\gamma_j-\gamma_g)+\frac{\theta_1\gamma_g^2}{2\theta_2(k-1)+\theta_1\gamma_g}\right\}.$$

Let

$$\chi(\gamma_g)=1-\frac{2\theta_2(k-1)}{2\theta_2(k-1)+\theta_1\gamma_g}$$

so that

$$\gamma_g\chi(\gamma_g) = \frac{\theta_1\gamma_g^2}{2\theta_2(k-1)+\theta_1\gamma_g} \le \frac{\theta_1(k-1)}{2\theta_2+\theta_1}$$

and both $\chi(\gamma_g)$ and $\gamma_g\chi(\gamma_g)$ are increasing functions of γ_g. Since $\gamma_i+\gamma_j \le 2(k-1)$, we have

$$\begin{aligned}\theta_1(k-1)^2 &< \frac{\gamma_g\chi(\gamma_g)}{q_1q_2}\{2(2(k-1)-\gamma_g)+\gamma_g\chi(\gamma_g)\}\\ &< \frac{\chi(\gamma_g)}{q_1q_2}\{2\gamma_g(2(k-1)-\gamma_g)+\gamma_g^2\chi(\gamma_g)\}.\end{aligned}$$

We see that $\gamma_g(2(k-1)-\gamma_g)$ is an increasing function of γ_g since $\gamma_g \le k-1$. Therefore the right hand side of the above inequality is an increasing function of γ_g. Hence we obtain

$$\begin{aligned}\theta_1 &< \frac{\theta_1/(k-1)^2}{q_1q_2(2\theta_2+\theta_1)}\left\{2(k-1)^2+\frac{\theta_1(k-1)^2}{2\theta_2+\theta_1}\right\}\\ &= \frac{\theta_1}{q_1q_2(2\theta_2+\theta_1)}\left\{2+\frac{\theta_1}{2\theta_2+\theta_1}\right\}.\end{aligned}$$

Thus $(2\theta_2+\theta_1)^2 < (3\theta_1+4\theta_2)/q_1q_2$. Then we derive

$$\left(2\theta_2+\theta_1-\frac{1}{q_1q_2}\right)^2 < \frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}.$$

Thus we get either

$$2\theta_2+\theta_1 < \frac{1}{q_1q_2} \quad \text{or} \quad 2\theta_2+\theta_1-\frac{1}{q_1q_2} < \sqrt{\frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}},$$

giving (3.5). Further, from (3.14), we have

$$d_1 < \frac{\theta_1(\gamma_g-\gamma_h)^2}{q_1(2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h))} < \frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)}.$$

As in Case I, we have $d_2 < 4(k-1)/q_2$. Thus (3.6) follows. ∎

Let θ_1, θ_2 be as in the statement of Lemma 3.1.

COROLLARY 3.2. *We have*

$$\theta_1 < \frac{3}{q_1q_2}, \quad \theta_1+\theta_2 < \theta_1+2\theta_2 < \frac{3}{q_1q_2}. \tag{3.18}$$

Proof. Since $\theta_2 > 0$, we see from (3.5) that either

$$\theta_1 < \frac{1}{q_1q_2} \quad \text{or} \quad \left(\theta_1-\frac{1}{q_1q_2}\right)^2 < \frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2},$$

giving $\theta_1 < 3/q_1q_2$. Hence we deduce from (3.5) that

$$\theta_1 + 2\theta_2 < \frac{1}{q_1q_2} + \sqrt{\frac{1}{(q_1q_2)^2} + \frac{\theta_1}{q_1q_2}} < \frac{3}{q_1q_2}.$$

Thus (3.18) is valid. ∎

LEMMA 3.3. *Let* $b_i = b_j$, $b_g = b_h$ *and* $(d_1, d_2) \neq (\eta, d/\eta)$ *be a partition of* d. *Suppose that* (i,j) *and* (g,h) *correspond to the partitions* (d_1, d_2) *and* (d_2, d_1), *respectively. Then*

$$d_1 < \eta(k-1)^2, \quad d_2 < \eta(k-1)^2. \tag{3.19}$$

Proof. We write

$$y_i - y_j = d_1r_1, \quad y_i + y_j = d_2r_2, \quad y_g - y_h = d_2s_2, \quad y_g + y_h = d_1s_1$$

with

$$b_ir_1r_2 = \gamma_i - \gamma_j, \quad b_gs_1s_2 = \gamma_g - \gamma_h. \tag{3.20}$$

Then as in the proof of Lemma 3.1, we get (3.7) and (3.8). If both $b_ir_1^2 - b_gs_1^2 \neq 0$ and $b_ir_2^2 - b_gs_2^2 \neq 0$, we obtain $\max(d_1, d_2) < \eta\max(b_ir_1^2, b_gs_1^2, b_ir_2^2, b_gs_2^2) \le \eta(k-1)^2$ by (3.20). Thus we may assume that either $b_ir_1^2 - b_gs_1^2 = 0$ or $b_ir_2^2 - b_gs_2^2 = 0$. Note that $b_ir_1^2 - b_gs_1^2 = b_ir_2^2 - b_gs_2^2 = 0$ is not possible. Suppose $b_ir_1^2 - b_gs_1^2 = b_ir_2^2 - b_gs_2^2 = 0$. Then $b_i = b_g$, $r_1 = s_1$, $r_2 = s_2$, implying $y_i = y_g$, $y_j = y_h$. Hence we get $\gamma_i = \gamma_g, \gamma_j = \gamma_h$ from (2.2), whence $(i,j) = (g,h)$, which is a contradiction. Now we consider the case $b_ir_1^2 - b_gs_1^2 = 0$; the proof for the other is similar. From $b_ir_2^2 - b_gs_2^2 \neq 0$ and (3.7), we obtain $2(\gamma_i + \gamma_j - \gamma_g - \gamma_h)d_1 = (b_ir_2^2 - b_gs_2^2)d_2$, which implies $d_1 \mid \eta(b_ir_2^2 - b_gs_2^2)$ and $d_2 \mid 2\eta(\gamma_i + \gamma_j - \gamma_g - \gamma_h)$. Hence by (3.20), $d_1 < \eta(k-1)^2$, $d_2 < 2\eta(k-1+k-2-1) \le \eta(k-1)^2$, implying (3.19). ∎

For two pairs $(a,b), (c,d)$ with positive rationals a,b,c,d, we write $(a,b) \ge (c,d)$ if $a \ge c$, $b \ge d$.

LEMMA 3.4. *Let* (d_1, d_2) *be a partition of* d. *Suppose that there is a set* $\mathfrak{G}$ *of at least* z_0 *distinct pairs corresponding to the partition* (d_1, d_2) *such that* $V(i,j,g,h,d_1,d_2)$ *is non-degenerate for any* (i,j) *and* (g,h) *in* $\mathfrak{G}$. *Then* (3.5), (3.6) *and* (3.18) *hold with* $(q_1, q_2) \ge (Q_1, Q_2)$ *where* (Q_1, Q_2) *is given by Table* 1.

Table 1

z_0	d odd	$2 \parallel d$	$4 \parallel d$	$8 \mid d$
2	$(1,1)$	$(2,1)$	$(1/2,1/2)$	$(1,1/2)$ if $2 \parallel d_1$, $(1/2,1)$ if $2 \parallel d_2$
3	$(2,2)$	$(4,4)$ or $(8,2)$	$(2,2)$	$(2,2)$
5	$(4,4)$	$(8,4)$	$(2,8)$ or $(8,2)$	$(2,8)$ if $2 \parallel d_1$, $(8,2)$ if $2 \parallel d_2$

For example, $(Q_1, Q_2) = (1, 1)$ if $z_0 = 2$, d odd, and $(Q_1, Q_2) = (2, 2)$ if $z_0 = 3$, $4 \parallel d$. If there exists a non-degenerate double pair $V(i, j, g, h, d_1, d_2)$, then we can apply Lemma 3.4 with $z_0 = 2$.

Proof of Lemma 3.4. For any pair $(i, j) \in \mathfrak{G}$, we write

$$y_i - y_j = r_1(i, j)d_1 \quad \text{and} \quad y_i + y_j = r_2(i, j)d_2 \tag{3.21}$$

where $r_1 = r_1(i, j)$ and $r_2 = r_2(i, j)$ are integers.

Let d be odd. Then $r_1 \equiv r_2 \pmod 2$ for any pair (i, j) by (3.21) and we shall use it in this paragraph without reference. We observe that $q_1 \geq 1$, $q_2 \geq 1$ by (3.8), (3.4) and the assertion follows for $z_0 = 2$. Let $z_0 = 3$. If there are two distinct pairs (i, j) with $b_i r_1$ even, then $q_1 \geq 2, q_2 \geq 2$ by (3.8). Thus we may assume that there is at most one pair (i, j) for which $b_i r_1$ is even. Therefore, for the remaining two pairs, we see that both $b_i r_1$'s are odd and the assertion follows again by (3.8). Let $z_0 = 5$. We may suppose that there is at most one (i, j) for which r_1 is even, otherwise the result follows from (3.8). Now we consider the remaining four pairs (i, j) for which $r_1^2 \equiv 1 \pmod 4$. Among these pairs, there are (i_1, j_1) and (i_2, j_2) such that $b_{i_1} \equiv b_{i_2} \pmod 4$ since b's are squarefree. Now the assertion follows from (3.8).

Let d be even. We observe that

$$8 \mid (y_i^2 - y_j^2) \quad \text{and} \quad \gcd(y_i - y_j, y_i + y_j) = 2 \tag{3.22}$$

for any pair (i, j). Let $2 \parallel d$. Then d_1 is odd and d_2 is even, implying r_1 is even by (3.22). Further, from (3.22), we have either $4 \mid r_1,\ 2 \nmid r_2$ or $2 \parallel r_1,\ 2 \mid r_2$. Therefore $(q_1, q_2) \geq (2, 1)$ by (3.8) since r_1 is even and the assertion follows for $z_0 = 2$. Let $z_0 = 3$. Then there are two pairs (i_1, j_1) and (i_2, j_2) such that $r_2(i_1, j_1) \equiv r_2(i_2, j_2) \pmod 2$. Assume that r_2 is odd. Then $4 \mid r_1$, which implies $8 \mid q_1$ and $2 \mid q_2$ by (3.8). Now we suppose that r_2 is even. Then $2 \parallel r_1$. We write $r_1 = 2r_1'$ and

$$b_{i_1} r_1^2(i_1, j_1) - b_{i_2} r_1^2(i_2, j_2) = 4(b_{i_1} r_1'^2(i_1, j_1) - b_{i_2} r_1'^2(i_2, j_2)) \equiv 0 \pmod 8.$$

Hence $4 \mid q_1$, $4 \mid q_2$ by (3.8). Let $z_0 = 5$. We choose three pairs (i, j) for which all $b_i \equiv 1 \pmod 4$ or all $b_i \equiv 3 \pmod 4$. From these, we choose two pairs both of which satisfy either $4 \mid r_1,\ 2 \nmid r_2$ or $2 \parallel r_1,\ 2 \mid r_2$. Now we argue as above and use $b_{i_1} \equiv b_{i_2} \pmod 4$ to get the result.

Let $4 \parallel d$. Then both d_1 and d_2 are even. From (3.22), we have either $2 \mid r_1$, $2 \nmid r_2$ or $2 \nmid r_1$, $2 \mid r_2$. Since $(q_1, q_2) \geq (1/2, 1/2)$ by (3.8), the assertion follows for $z_0 = 2$. Let $z_0 = 3$. Then there are two pairs (i_1, j_1) and (i_2, j_2) such that $r_1(i_1, j_1) \equiv r_1(i_2, j_2) \pmod 2$ and $r_2(i_1, j_1) \equiv r_2(i_2, j_2) \pmod 2$. Since $b_i \equiv n \pmod 4$ for each i, we deduce from (3.8) and (3.4) that $2 \mid q_1$ and $2 \mid q_2$. Thus $(q_1, q_2) \geq (2, 2)$. Let $z_0 = 5$. Then we get three pairs (i, j) for which $2 \mid r_1(i, j), 2 \nmid r_2(i, j)$ or three pairs (i, j) for which $2 \nmid r_1(i, j), 2 \mid r_2(i, j)$. Assume the first case. Then there are two pairs (i_1, j_1) and (i_2, j_2) such that

$r_1(i_1,j_1)\equiv r_1(i_2,j_2)\pmod 4$. This, with $b_i\equiv n\pmod 4$ and (3.4), implies that $16\mid q_1d_2$ and $4\mid q_2d_1$. Hence $(q_1,q_2)\ge(8,2)$. In the latter case, we get $(q_1,q_2)\ge(2,8)$ similarly.

Let $8\mid d$. Then we see from (3.21) and (3.22) that either $2\parallel d_1$, implying all r_1's are odd, or $2\parallel d_2$, implying all r_2's are odd. Also, $b_i\equiv n\pmod 8$ for all i. We prove the result for $2\parallel d_1$; the proof for the other case is similar. From (3.7), we derive

$$(3.23)\quad 2(\gamma_{i_1}+\gamma_{j_1}-\gamma_{i_2}-\gamma_{j_2})\frac{d_1}{2}\frac{d_2}{2} = (b_{i_1}r_1^2-b_{i_2}s_1^2)\left(\frac{d_1}{2}\right)^2+(b_{i_1}r_2^2-b_{i_2}s_2^2)\left(\frac{d_2}{2}\right)^2$$

where $r_1=r_1(i_1,j_1)$, $s_1=r_1(i_2,j_2)$, $r_2=r_2(i_1,j_1)$ and $s_2=r_2(i_2,j_2)$. Noting that $4d_2\mid d_2^2$ and taking modulo d_2, we get $(q_1,q_2)\ge(1,1/2)$, whence the assertion for $z_0=2$. Let $z_0=3$. Then there are two pairs (i_1,j_1) and (i_2,j_2) such that $r_2(i_1,j_1)\equiv r_2(i_2,j_2)\pmod 2$. Using this and (3.4), we get $4\mid q_2d_1$. Further, from $b_ir_1r_2=\gamma_i-\gamma_j$, we see that $\gamma_{i_1}-\gamma_{j_1}\equiv\gamma_{i_2}-\gamma_{j_2}\pmod 2$, hence $\gamma_{i_1}+\gamma_{j_1}\equiv\gamma_{i_2}+\gamma_{j_2}\pmod 2$. Now we see from (3.23) that $4(d_2/2)\mid q_1d_2$. Thus $(q_1,q_2)\ge(2,2)$. Let $z_0=5$. We see that $b_i\equiv n$ or $n+8$ modulo 16, so that $b_ir_2^2\pmod{16}$ is equal to 0 if $4\mid r_2$, $4n$ if $2\parallel r_2$, and n or $n+8$ if $2\nmid r_2$. Now we can find two pairs (i_1,j_1) and (i_2,j_2) such that $b_{i_1}r_2^2(i_1,j_1)\equiv b_{i_2}r_2^2(i_2,j_2)\pmod{16}$. This gives $16\mid q_2d_1$ by (3.4). Further, again $2\mid(\gamma_{i_1}+\gamma_{j_1}-\gamma_{i_2}-\gamma_{j_2})$ and hence $4(d_2/2)\mid q_1d_2$ from (3.23). Therefore $(q_1,q_2)\ge(2,8)$. ■

LEMMA 3.5.

(i) *Assume that*

$$(3.24)\qquad n+\gamma_td>\eta^2\gamma_t^2.$$

Then for any pair (i,j) with $b_i=b_j$, the partition $(d\eta^{-1},\eta)$ is not possible.

(ii) *Let $d=d'd''$ with $\gcd(d',d'')=1$. Then for any pair (i,j) with $B_i=B_j\ge d'$, $i,j\in T_1$, the partition $(d''\eta^{-1},\eta)$ is not possible. In particular, the partition $(d\eta^{-1},\eta)$ is not possible.*

Proof. (i) Suppose the pair (i,j) with $b_i=b_j$ corresponds to the partition $(d\eta^{-1},\eta)$. From $(n+\gamma_id)/(n+\gamma_td)>\gamma_i/\gamma_t$ and (3.24), we get $n+\gamma_id>\eta^2\gamma_i\gamma_t$. Then from (2.8), we have

$$\gamma_i-\gamma_j\ge\frac{b_i(y_i+y_j)}{\eta}\ge\frac{(b_iy_i^2)^{1/2}+(b_jy_j^2)^{1/2}}{\eta}>\frac{\eta(\sqrt{\gamma_i\gamma_t}+\sqrt{\gamma_j\gamma_t})}{\eta}\ge\gamma_i+\gamma_j,$$

a contradiction.

(ii) Suppose the pair (i,j) with $B_i = B_j \geq d'$ corresponds to the partition $(d''\eta^{-1}, \eta)$. As in (2.8), we have

$$\gamma_i - \gamma_j \geq (\gamma_i - \gamma_j)\,\frac{d'}{B_i} \geq \frac{Y_i + Y_j}{\eta} > \frac{2k}{2}$$

since $Y_i \geq Y_j > k$. This is a contradiction. The last assertion follows by taking $d' = 1,\ d'' = d$. ∎

Lemma 3.6.

(i) *Assume* (3.24). *Let* $1 \leq i_0 \leq t$ *and* $\nu(b_{i_0}) = \mu$. *Let* (d_1, d_2) *be any partition of* d. *Then the number of pairs* (i,j) *with* $b_i = b_j = b_{i_0}$, $i > j$, *corresponding to* (d_1, d_2) *is at most* $[\mu/2]$.

(ii) *Let* $d = d'd''$ *with* $\gcd(d', d'') = 1$. *Let* $i_0 \in T_1$, $B_{i_0} \geq d'$ *and* $\nu(B_{i_0}) = \mu$. *Let* (d_1, d_2) *be any partition of* d''. *Then the number of pairs* (i,j) *with* $B_i = B_j = B_{i_0}$, $i > j$, *corresponding to* (d_1, d_2) *is at most* $[\mu/2]$.

Proof. (i) Suppose there are $\mu' = [\mu/2] + 1$ pairs (i_l, j_l) with $i_l > j_l$, $0 \leq l < \mu'$ and $b_{i_l} = b_{j_l} = b_{i_0}$ corresponding to (d_1, d_2). We consider the sets $I = \{i_l : 0 \leq l < \mu'\}$ and $J = \{j_l : 0 \leq l < \mu'\}$. If $|I| < \mu'$ or $|J| < \mu'$ or $I \cap J \neq \emptyset$, then there are $l \neq m$ such that

$$\begin{aligned} &d_1 \mid (y_{j_l} - y_{j_m}), \quad d_2 \mid (y_{j_l} - y_{j_m}) \quad \text{if } i_l = i_m,\\ &d_1 \mid (y_{i_l} - y_{i_m}), \quad d_2 \mid (y_{i_l} - y_{i_m}) \quad \text{if } j_l = j_m,\\ &d_1 \mid (y_{j_l} - y_{i_m}), \quad d_2 \mid (y_{j_l} - y_{i_m}) \quad \text{if } i_l = j_m. \end{aligned}$$

We exclude the first possibility; the proofs for the others are similar. Without loss of generality, we may assume that $j_l > j_m$. Then $\operatorname{lcm}(d_1, d_2) \mid (y_{j_l} - y_{j_m})$ so that the pair (j_l, j_m) corresponds to the partition $(d\eta^{-1}, \eta)$. This is not possible by Lemma 3.5(i). Thus $|I| = \mu'$, $|J| = \mu'$ and $I \cap J = \emptyset$. Now we see that $|I \cup J| = |I| + |J| = 2\mu' > \mu$ and $b_i = b_{i_0}$ for every $i \in I \cup J$. This contradicts $\nu(b_{i_0}) = \mu$.

(ii) The proof is similar to that of (i); we use Lemma 3.5(ii). ∎

As a corollary, we have

Corollary 3.7.

(i) *Assume* (3.24). *For* $1 \leq i \leq t$, *we have* $\nu(b_i) \leq 2^{\omega(d)-\theta}$.

(ii) *Let* $d = d'd''$ *with* $\gcd(d', d'') = 1$. *For* $B_i \geq d'$, *we have* $\nu(B_i) \leq 2^{\omega(d'')-\theta_1}$. *In particular*, $\nu(B_i) \leq 2^{\omega(d)-\theta}$.

Proof. (i) Let $\nu(b_i) = \mu$. Then there are $\mu(\mu-1)/2$ pairs (g,h) with $g > h$ and $b_g = b_h = b_i$. Since there are at most $2^{\omega(d)-\theta} - 1$ permissible partitions of d, we see from Lemma 3.6(i) that $\mu(\mu-1)/2 \leq (\mu/2)(2^{\omega(d)-\theta} - 1)$. Hence the assertion follows.

(ii) The proof is similar; we use Lemma 3.6(ii). ∎

COROLLARY 3.8. *Let $T_{r+1}=\{i\in T_1 : B_i\ge \mathfrak{q}_1\cdots\mathfrak{q}_r\}$ and $s_{r+1}=|\{B_i : i\in T_{r+1}\}|$. Then*

$$s_{r+1}\ge \frac{|T_1|}{2^{\omega(d)-r-\theta}}-\sum_{\mu=1}^{r-1}2^{r-\mu}\lambda_\mu-2\lambda_r$$

where λ's are as defined in (2.10).

Proof. We apply Corollary 3.7(ii) with $d'=\mathfrak{q}_1\cdots\mathfrak{q}_\mu$ to derive that $\nu(B_i)\le 2^{\omega(d)-\mu-\theta}$ for $B_i\ge\mathfrak{q}_1\cdots\mathfrak{q}_\mu$, $\mu\ge 1$ since $\theta_1\ge\theta$. Therefore

$$|T_{r+1}| \ge |T_1|-2^{\omega(d)-\theta}\lambda_1-2^{\omega(d)-1-\theta}(\lambda_2-\lambda_1)-\cdots-2^{\omega(d)-r+1-\theta}(\lambda_r-\lambda_{r-1}).$$

Since $\nu(B_i)\le 2^{\omega(d)-r-\theta}$ for $i\in T_{r+1}$, we have $s_{r+1}\ge|T_{r+1}|/2^{\omega(d)-r-\theta}$ and the assertion follows. ∎

LEMMA 3.9. *Assume* (3.24). *There exists a set Ω of at least*

$$t-|R|+\sum_{\substack{\mu>1\\ \mu\ odd}}r_\mu\ge t-|R|$$

pairs (i,j) having Property ND.

Proof. We have

$$t=\sum_\mu \mu r_\mu \quad\text{and}\quad |R|=\sum_\mu r_\mu.$$

Each $b_{i_0}\in R_\mu$ gives rise to $\mu(\mu-1)/2$ pairs (i,j) with $i>j$ such that $b_i=b_j=b_{i_0}$ and each pair corresponds to a partition of d. By Lemma 3.6, we know that there are at most $[\mu/2]$ pairs corresponding to any partition of d. For each $1\le j\le[\mu/2]=\mu_1$, let v_j be the number of partitions of d for which there are j pairs out of the ones given by $b_{i_0}\in R_\mu$ corresponding to that partition. Then

$$\frac{\mu(\mu-1)}{2}=\sum_{j=1}^{\mu_1}jv_j. \tag{3.25}$$

For each partition having j pairs with $v_j>0$, we remove $j-1$ pairs. Thus we remove in all $\sum_{j=1}^{\mu_1}(j-1)v_j$ pairs. Rewriting (3.25) as

$$\frac{\mu(\mu-1)}{2}=\mu_1\sum_{j=1}^{\mu_1}v_j-\sum_{j=1}^{\mu_1}(\mu_1-j)v_j,$$

we see that we are left with at least

$$\sum_{j=1}^{\mu_1}v_j=\frac{\mu(\mu-1)}{2\mu_1}+\sum_{j=1}^{\mu_1}\left(1-\frac{j}{\mu_1}\right)v_j\ge\frac{\mu(\mu-1)}{2\mu_1}=\begin{cases}\mu-1 & \text{if } \mu \text{ is even,}\\ \mu & \text{if } \mu \text{ is odd}\end{cases}$$

pairs. Let Ω be the union of all such pairs taken over all $b_{i_0} \in R_\mu$ and for all $\mu \geq 2$. Since $|R_\mu| = r_\mu$, we have

$$|\Omega| \geq \sum_{\mu \text{ even}} (\mu - 1) r_\mu + \sum_{\substack{\mu > 1 \\ \mu \text{ odd}}} \mu r_\mu = t - |R| + \sum_{\substack{\mu > 1 \\ \mu \text{ odd}}} r_\mu.$$

Further, we see from the construction of the set Ω that Ω has Property ND. ∎

Corollary 3.10. *Assume* (3.24)*. Let z be a positive integer and* $\mathfrak{h}(z) = (z-1)(2^{\omega(d)-\theta} - 1) + 1$*. Let* $z_0 \in \{2, 3, 5\}$*. Suppose that* $t - |R| \geq \mathfrak{h}(z_0)$*. Then there exists a partition* (d_1, d_2) *of d such that* (3.5), (3.6) *and* (3.18) *hold with* $(q_1, q_2) \geq (Q_1, Q_2)$ *where* (Q_1, Q_2) *is given by Table* 1.

Proof. By Lemma 3.9, there exists a set Ω with at least $\mathfrak{h}(z_0)$ pairs having Property ND. Since there are at most $2^{\omega(d)-\theta} - 1$ permissible partitions of d by Lemma 3.5(i), we can find a partition (d_1, d_2) of d and a subset $\mathfrak{G} \subset \Omega$ of at least z_0 pairs corresponding to (d_1, d_2). Now the result follows by Lemma 3.4. ∎

Corollary 3.11. *Assume* (3.24)*. Suppose that* $t - |R| \geq 2^{\omega(d)-\theta-1} + 1$*. Then there exists a partition* (d_1, d_2) *of d such that* (3.19) *holds.*

Proof. By Lemma 3.9, there exists a set Ω with at least $2^{\omega(d)-\theta-1} + 1$ pairs (i, j) having Property ND. We may assume that for each partition (d_1, d_2) of d, there is at most one pair corresponding to (d_1, d_2), otherwise the assertion follows by taking $z_0 = 2$ in Lemma 3.4. We see that there are $2^{\omega(d)-\theta-1} - 1$ partitions (d_1, d_2) with $d_1 > d_2$, $2^{\omega(d)-\theta-1} - 1$ partitions (d_1, d_2) with $\eta < d_1 < d_2$ and the partition $(\eta, d\eta^{-1})$. Since there are at least $2^{\omega(d)-\theta-1} + 1$ pairs, we can find two pairs (i, j) and (g, h) corresponding to the partitions (d_1, d_2) and (d_2, d_1), respectively. Now the assertion follows by Lemma 3.3. ∎

Lemma 3.12. *Assume* (3.24).

(i) *Let* $|S_1| \leq |T_1| - \mathfrak{h}(3)$*. Then* (3.18) *is valid with*

$$q_1 q_2 \geq \begin{cases} 144\varrho^{-1} & \text{if } 2 \nmid d, \\ 16 & \text{if } 2 \parallel d, \\ 4 & \text{if } 4 \mid d. \end{cases} \tag{3.26}$$

(ii) *Let d be even and* $|S_1| \leq |T_1| - \mathfrak{h}(5)$*. Then* (3.18) *is valid with*

$$q_1 q_2 \geq \begin{cases} 144\varrho^{-1} & \text{if } 2 \parallel d, \\ 36 & \text{if } 4 \mid d \text{ and } 3 \nmid d, \\ 16 & \text{if } 4 \mid d \text{ and } 3 \mid d. \end{cases} \tag{3.27}$$

Proof. Let $B_i = B_j$ with $i > j$ and $i, j \in T_1$. Then there is a partition (d_1, d_2) of d such that $Y_i - Y_j = d_1 r_1'$, $Y_i + Y_j = d_2 r_2'$ with r_1', r_2' even, $24\varrho^{-1} \mid r_1' r_2'$ if d is odd and r_1' even, $12\varrho^{-1} \mid r_1' r_2'$ if $2 \parallel d$ and $3\varrho^{-1} \mid r_1' r_2'$ if $4 \mid d$. Since $B_i Y_i^2 = b_i y_i^2$ and b_i is squarefree, we see that $p \mid b_i$ if and only if $p \mid B_i$ with $\mathrm{ord}_p(B_i)$ odd. Therefore $b_i = b_j$ implying $b^2 = B_i/b_i = B_j/b_j$ and $y_i = bY_i$, $y_j = bY_j$. Hence

$$y_i - y_j = d_1 b r_1' = d_1 r_1(i,j) = d_1 r_1, \quad y_i + y_j = d_2 b r_2' = d_2 r_2(i,j) = d_2 r_2$$

with $r_1 = br_1'$, $r_2 = br_2'$ even, $24\varrho^{-1} \mid r_1 r_2$ if d is odd, and with r_1 even, $12\varrho^{-1} \mid r_1 r_2$ if $2 \parallel d$ and $3\varrho^{-1} \mid r_1 r_2$ if $4 \mid d$. Let $z \in \{3, 5\}$ and $|S_1| \le |T_1| - \mathfrak{h}(z)$. We argue as in Lemma 3.9 and Corollary 3.10 with t and $|R|$ replaced by $|T_1|$ and $|S_1|$. There exists a partition (d_1, d_2) of d and z pairs corresponding to (d_1, d_2) such that $V(i, j, g, h, d_1, d_2)$ is non-degenerate for any two such distinct pairs (i, j) and (g, h). Let $z = 3$. By Lemma 3.4 with $z_0 = 3$, we may suppose that d is odd. Let $3 \nmid d$. Then we can find two distinct pairs (i_1, j_1) and (i_2, j_2) both of which satisfy either $3 \mid r_1(i_1, j_1)$, $3 \mid r_1(i_2, j_2)$ or $3 \mid r_2(i_1, j_1)$, $3 \mid r_2(i_2, j_2)$. Now (3.26) follows from (3.8) and (3.4) since r_1, r_2 are even. Assume that $3 \mid d$. Let $3 \mid d_1$. Then we can find two distinct pairs (i_1, j_1) and (i_2, j_2) both of which satisfy either $3 \mid r_1(i_1, j_1)$, $3 \mid r_1(i_2, j_2)$ or $3 \nmid r_1(i_1, j_1)$, $3 \nmid r_1(i_2, j_2)$. Since $b_i \equiv n \pmod 3$ and $r^2 \equiv 1 \pmod 3$ for $3 \nmid r$, the assertion follows from (3.8) and (3.4) since r_1, r_2 are even. The same assertion holds for $3 \mid d_2$, in which case r_1 is replaced by r_2. This proves (3.26).

Now we turn to the proof of (3.27). Let d be even and $z = 5$. Let $3 \nmid d$. Out of these five pairs, we can find three distinct pairs (i, j) for which either $r_1(i, j)$'s are all divisible by 3 or $r_2(i, j)$'s are all divisible by 3. As in the proof of Lemma 3.4 with d even and $z_0 = 3$, we find two distinct pairs (i_1, j_1) and (i_2, j_2) such that $16 \mid q_1 q_2$ if $2 \parallel d$ and $4 \mid q_1 q_2$ if $4 \mid d$. Further, $9 \mid q_1 q_2$ since either $r_1(i, j)$'s are all divisible by 3 or $r_2(i, j)$'s are all divisible by 3 and hence the assertion. Assume now that $3 \mid d$. By Lemma 3.4 with $z_0 = 5$, we may suppose that $2 \parallel d$. Let $3 \mid d_1$. Then we can find three pairs (i, j) for which either 3 divides all $r_1(i, j)$'s or 3 does not divide any $r_1(i, j)$. Then for any two such pairs (i_1, j_1) and (i_2, j_2), we have $3 \mid (b_{i_1} r_1^2(i_1, j_1) - b_{i_2} r_1^2(i_2, j_2))$. Therefore, by the proof of Lemma 3.4 with d even and $z_0 = 3$, we get $3 \cdot 16 \mid q_1 q_2$. The other case $3 \mid d_2$ is similar. ■

4. Lower bound for $n + (k-1)d$. We observe that $|S_1| \ge |T_1|/2^{\omega(d)-\theta}$ and $n + (k-1)d \ge |S_1| k^2$. We give a lower bound for $|T_1|$. We have

LEMMA 4.1. *Let $k \ge 4$. Then*

$$(4.1) \qquad |T_1| > t - \frac{(k-1)\log(k-1) - \sum_{p \mid d,\, p<k} \max(0, \frac{(k-1-p)\log p}{p-1} - \log(k-2))}{\log(n + (k-1)d)} - \pi_d(k) - 1.$$

Proof. The proof depends on an idea of Sylvester and Erdős and is similar to [SaSh03a, Lemma 3]. Since $|T_1| = t - |T|$, we may assume that $|T| > \pi_d(k)$. For a prime q with $q \le k$ and $q \nmid d$, let i_q be a term such that $\mathrm{ord}_q(B_{i_q})$ is maximal. Let $T' = T \setminus \{i_q : q \le k,\ q \nmid d\}$. Thus $|T'| \ge |T| - \pi_d(k)$. Let $i \in T'$. Then $n + \gamma_i d = B_i$ and $\mathrm{ord}_q(n + \gamma_i d) \le \mathrm{ord}_q(\gamma_i - \gamma_{i_q})$ since $\gcd(n, d) = 1$. Therefore

$$\mathrm{ord}_q\Big(\prod_{i\in T'}(n+\gamma_i d)\Big) \le \mathrm{ord}_q(\gamma_{i_q}!(k-1-\gamma_{i_q})!) \le \mathrm{ord}_q(k-1)!.$$

This, with $n + id \ge \frac{i}{k-1}(n + (k-1)d)$ for $i > 0$, gives

$$(|T'|-1)!\Big(\frac{n+(k-1)d}{k-1}\Big)^{|T'|-1} < \prod_{i\in T'}(n+\gamma_i d) \le (k-1)!\psi^{-1}$$

where $\psi = \prod_{q|d} q^{\mathrm{ord}_q(k-1)!}$. Therefore

$$\begin{aligned}(|T| - \pi_d(k) - 1)\log(n+(k-1)d) & \\ &< (|T'|-1)\log(k-1) + \log((k-1)\cdots|T'|) - \log\psi \\ &\le (k-1)\log(k-1) - \log\psi.\end{aligned}$$

Now the assertion (4.1) follows from Lemma 5.1(iv) below. ∎

The following result is an immediate consequence of Laishram and Shorey [LaSh06, Theorem 1].

LEMMA 4.2. *Let $n \ge 1, d > 2$ and $k \ge 5$. Then*

$$P(n(n+d)\cdots(n+(k-1)d)) > 2k \tag{4.2}$$

unless $(n, d, k) = (1, 3, 10)$.

LEMMA 4.3. *Let $t = k$. Then*

$$|T_1| > \alpha k \quad \text{for } k \ge K_\alpha \tag{4.3}$$

where α and K_α are given by

α	0.3	0.35	0.4	0.42
K_α	101	203	710	1639

Proof. Let $k \ge K_\alpha$. Thus $k \ge 101$. By Lemma 4.2, $n + (k-1)d > 4k^2$. We see from (4.1) that

$$|T_1| + \pi_d(k) > k - 1 - \frac{(k-1)\log k}{2\log 2k} = \frac{k}{2} + \frac{1}{2}\Big\{\frac{(k-1)\log 2}{\log 2k} - 1\Big\} > \frac{k}{2}.$$

Therefore $n + (k-1)d > \big(\frac{k}{2}\log\frac{k}{2}\big)^2$ by Lemma 5.1(ii).

For $0 < \beta < 1$, let

$$n + (k-1)d > (\beta k \log \beta k)^2. \tag{4.4}$$

We may assume that $\beta \geq 1/2$. Put $X_\beta = X_\beta(k) = \beta \log \beta k$. Then $\log(n + (k-1)d) > 2\log X_\beta + 2\log k$. From (4.1), we see that

$$(4.5)\quad |T_1| + \pi_d(k) > k - 1 - \frac{(k-1)\log k}{2\log X_\beta + 2\log k} = \frac{k}{2}\left(1 - \frac{1}{k}\right)\left(1 + \frac{\log X_\beta}{\log X_\beta + \log k}\right) = \frac{k}{2}\left(1 - \frac{1}{k}\right)\left(1 + \frac{1}{1 + \frac{\log k}{\log X_\beta}}\right) =: g_\beta(k)k =: g_\beta k.$$

By using $\pi_d(k) \leq \pi(k)$ and Lemma 5.1(i), from (4.5) we get

$$(4.6)\qquad |T_1| > g_\beta k - \frac{k}{\log k}\left(1 + \frac{1.2762}{\log k}\right).$$

Let $\beta = 1/2$. We observe that

$$\frac{14}{13}\log k - \left(1 + \frac{\log k}{\log X_\beta}\right)\left(1 + \frac{1.2762}{\log k}\right) = \left(\frac{14}{13} - \frac{1}{\log X_\beta}\right)\log k - \left(\frac{1.2762}{\log k} + \frac{1.2762}{\log X_\beta}\right) - 1$$

is an increasing function of k and it is positive at $k = 2500$. Therefore

$$\frac{1}{1 + \frac{\log k}{\log X_\beta}} > \frac{13}{14}\frac{1}{\log k}\left(1 + \frac{1.2762}{\log k}\right) \quad \text{for } k \geq 2500,$$

which, together with (4.6) and (4.5), implies

$$\frac{|T_1|}{k} > \frac{1}{2} - \frac{1}{2k} - \frac{1}{28\log k}\left(1 + \frac{1.2762}{\log k}\right)\left(15 + \frac{13}{k}\right) > 0.42 \quad \text{for } k \geq 2500$$

since the middle expression is an increasing function of k. Thus we may suppose that $k < 2500$. From (4.5), we get $|T_1| + \pi_d(k) > g_{1/2}k =: \beta_1 k$. Then (4.4) is valid with β replaced by β_1 and we deduce from (4.5) that $|T_1| + \pi_d(k) > g_{\beta_1}k =: \beta_2 k$. We iterate this process with β replaced by β_2 to get $g_{\beta_2} =: \beta_3$ and further with β_3 to get $|T_1| + \pi_d(k) > g_{\beta_3}k =: \beta_4 k$. Finally we see that $|T_1| > \beta_4 k - \pi(k) \geq \alpha k$ for $k \geq K_\alpha$. ∎

LEMMA 4.4. *Let $S \subseteq \{B_i : 1 \leq i \leq t\}$. Let $h \geq 1$ and $P_1 < \cdots < P_h$ be a subset of odd primes dividing d. For $|S| > ((P_1-1)/2)\cdots((P_h-1)/2)$, we have*

$$(4.7)\qquad \max_{B_i \in S} B_i \geq \begin{cases} \frac{3}{4}\cdot 2^{h+\delta}|S| & \text{if } 3 \nmid d, \\ \frac{9}{8}\cdot 2^{h+\delta}|S| & \text{if } 3 \mid d. \end{cases}$$

Proof. The assertion (4.7) for $3 \nmid d$ is [Lai06, Corollary 2] with A_i replaced by B_i and $s = |S|$. Let $3 \mid d$. As in [Lai06, Corollary 2], let $Q_h \geq 1$ and

$1 \le f \le (P_h - 1)/2$ be integers such that

$$(f-1)\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right) < |S| - Q_h\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_h-1}{2}\right) \le f\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{t-1}-1}{2}\right).$$

Then we continue the proof as in [Lai06, Corollary 2] to get

$$\max_{B_i \in S} B_i \ge 2^\delta Q_h P_1 \cdots P_h + 2^\delta (f-1) P_1 \cdots P_{h-1}.$$

Since $P_1 = 3$, it suffices to show

$$Q_h P_2 \cdots P_h + (f-1) P_2 \cdots P_{h-1} \ge \frac{3}{4}\{Q_h(P_2-1)\cdots(P_h-1) + 2f(P_2-1)\cdots(P_{h-1}-1)\}$$

to get the assertion (4.7). For $h = 2$, we see from

$$\frac{1}{4} Q_h(P_2+3) - 1 - \frac{f}{2} \ge \frac{1}{4} P_2 - \frac{1}{4} - \frac{P_2-1}{4} = 0$$

that the above inequality is valid. For $h \ge 3$, by observing that

$$Q_h(P_2-1)\cdots(P_h-1) \le Q_h P_2 \cdots P_h - Q_h P_2 \cdots P_{h-1},$$
$$2f(P_2-1)\cdots(P_{h-1}-1) \le 2f P_2 \cdots P_{h-1} - 2f P_2 \cdots P_{h-2},$$

it suffices to show that

$$Q_h + \frac{3(Q_h-1)-(2f+1)}{P_h} + \frac{6f}{P_h P_{h-1}} \ge 0,$$

which is true since $Q_h \ge 1$ and $1 \le f \le (P_h-1)/2$. ∎

COROLLARY 4.5. *We have* $\lambda_1 < \frac{2}{3}\mathfrak{q}_1$ *if* $2 \nmid d$, $3 \nmid d$ *and* $\lambda_1 < \mathfrak{q}_1/\varrho 2^\delta + 1$ *otherwise. For* $r \ge 2$, *we have*

$$\lambda_r < \begin{cases} \dfrac{\mathfrak{q}_1\cdots\mathfrak{q}_r}{3\cdot 2^{r-2}} & \text{if } 2\nmid d,\ 3\nmid d,\\ \dfrac{\mathfrak{q}_1\cdots\mathfrak{q}_r}{9\cdot 2^{r-3}} & \text{if } 2\nmid d,\ 3\mid d,\\ \dfrac{\mathfrak{q}_1\cdots\mathfrak{q}_r}{3\cdot 2^{\delta+r-3}} & \text{if } 2\mid d,\ 3\nmid d,\\ \min\left(\dfrac{\mathfrak{q}_1\cdots\mathfrak{q}_r}{3\cdot 2^{\delta}}+1, \dfrac{\mathfrak{q}_1\cdots\mathfrak{q}_r}{9\cdot 2^{r-2}}\right) & \text{if } 6\mid d. \end{cases}$$

Proof. Let $2 \nmid d$ and $3 \nmid d$. If $\lambda_r \ge \mathfrak{q}_1 \cdots \mathfrak{q}_r/(3 \cdot 2^{r-2})$, then

$$\lambda_r > \frac{\mathfrak{q}_1-1}{2}\cdots\frac{\mathfrak{q}_r-1}{2} \ge \frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_r-1}{2},$$

giving $\mathfrak{q}_1 \cdots \mathfrak{q}_r > \max_{B_i \in \mathcal{A}_r} B_i \ge \frac{3}{4} \cdot 2^r \lambda_r$ by (4.7) with $S = \mathcal{A}_r$. This is a contradiction.

Let $2\,|\,d$ or $3\,|\,d$. Then we derive from the Chinese remainder theorem that $\lambda_r < \mathfrak{q}_1\cdots\mathfrak{q}_r/\varrho 2^\delta + 1$. Thus we may suppose that $r \ge 2$. Further, we may also assume that $r \ge \delta + 1$ when $6\,|\,d$.

Let $2\nmid d$ and $3\,|\,d$. Suppose $\lambda_r \ge \mathfrak{q}_1\cdots\mathfrak{q}_r/(9\cdot 2^{r-3})$. Then $\mathfrak{q}_1 \ge \mathfrak{p}_1 = 3$, implying

$$\lambda_r > \frac{\mathfrak{q}_2-1}{2}\cdots\frac{\mathfrak{q}_r-1}{2} \ge \frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_r-1}{2}.$$

Therefore $\mathfrak{q}_1\cdots\mathfrak{q}_r > \frac{9}{4}\cdot 2^{r-1}\lambda_r$ by (4.7) with $S = \mathcal{A}_r$. This is a contradiction.

Let $2\,|\,d$ and $3\nmid d$. Suppose $\lambda_r \ge \mathfrak{q}_1\cdots\mathfrak{q}_r/(3\cdot 2^{\delta+r-3})$. Then $\mathfrak{q}_r \ge 7$ since $r \ge 2$, implying $\mathfrak{q}' := \max(\mathfrak{q}_r, 2^\delta) \ge 7$ and hence

$$\begin{aligned}\lambda_r &\ge \frac{2^{r-1}\mathfrak{q}'}{3\cdot 2^{\delta+r-3}}\,\frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-1}-1}{2} \ge \frac{\mathfrak{q}'}{6}\,\frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-1}-1}{2}\\ &> \frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-1}-1}{2}.\end{aligned}$$

Now we apply (4.7) with $S = \mathcal{A}_r$ to get a contradiction.

Let $6\,|\,d$. Suppose $\lambda_r \ge \mathfrak{q}_1\cdots\mathfrak{q}_r/(9\cdot 2^{r-2})$. Let $2\,\|\,d$ or $4\,\|\,d$. Then

$$\lambda_r > \frac{\mathfrak{q}_2-1}{2}\cdots\frac{\mathfrak{q}_{r-1}-1}{2} \ge \frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-2}-1}{2}$$

since $\mathfrak{q}_1\mathfrak{q}_r \ge 9$ and $\mathfrak{p}_1 = 3$, and (4.7) with $S = \mathcal{A}_r$ yields a contradiction. Thus it remains to consider $8\,|\,d$. Then

$$\lambda_r > \frac{\mathfrak{q}_2-1}{2}\cdots\frac{\mathfrak{q}_{r-1}-1}{2} \ge \frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-1}-1}{2}$$

since

$$\lambda_r \ge \frac{2^{r-2}\mathfrak{q}_1\mathfrak{q}'}{9\cdot 2^{r-2}}\,\frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-2}-1}{2} > \frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_{r-2}-1}{2}$$

where $\mathfrak{q}' := \max(\mathfrak{q}_r, 8)$, and (4.7) with $S = \mathcal{A}_r$ yields a contradiction. ∎

5. Results from other sources. We now state some lemmas. We begin with some estimates from prime number theory.

LEMMA 5.1. *We have*

(i) $\pi(x) \le \dfrac{x}{\log x}\left(1 + \dfrac{1.2762}{\log x}\right)$ *for* $x > 1$;

(ii) $p_i \ge i\log i$ *for* $i \ge 2$;

(iii) $\prod_{p\le x} p < 2.71851^x$ *for* $x > 0$;

(iv) $\sum_{p\le p_i} \log p > i(\log i + \log\log i - 1.076868)$ *for* $i \ge 2$;

(v) $\mathrm{ord}_p(k!) \ge \dfrac{k-p}{p-1} - \dfrac{\log(k-1)}{\log p}$ *for* $p < k$.

(i) is due to Dusart [Dus98, p. 14], [Dus99] and (ii) is proved by Rosser and Schoenfeld [RoSc62]. For estimate (iii) see [Dus98, Prop. 1.7], [Dus99]. Estimate (iv) is [Rob83, Theorem 6]. For a proof of (iv), see [LaSh04, Lemma 2(i)]. ■

The next lemma is Stirling's formula (see Robbins [Rob55]).

LEMMA 5.2. *For a positive integer* ν, *we have*

$$\sqrt{2\pi\nu}\, e^{-\nu}\nu^{\nu}e^{1/(12\nu+1)} < \nu! < \sqrt{2\pi\nu}\, e^{-\nu}\nu^{\nu}e^{1/(12\nu)}.$$

The following lemma is contained in [Lai06, Lemma 8].

LEMMA 5.3. *Let* s_i *denote the ith squarefree positive integer. Then*

$$\prod_{i=1}^{l} s_i \geq (1.6)^l l! \quad \text{for } l \geq 286. \tag{5.1}$$

Further, let t_i *be ith odd squarefree positive integer. Then*

$$\prod_{i=1}^{l} t_i \geq (2.4)^l l! \quad \text{for } l \geq 200. \tag{5.2}$$

The next result depends on an idea of Erdős and Rigge.

LEMMA 5.4. *Let* $z_1 > 1$ *be a real number*, $h_0 > i_0 \geq 0$ *be integers such that* $\prod_{b_i \in R} b_i \geq z_1^{|R|-i_0}(|R|-i_0)!$ *for* $|R| \geq h_0$. *Suppose that* $t - |R| < g$ *and let* $g_1 = k - t + g - 1 + i_0$. *For* $k \geq h_0 + g_1$ *and for any real number* $\mathfrak{m} > 1$, *we have*

$$g_1 > \frac{k \log\left(\frac{z_1 \mathfrak{n}_0}{2.71851} \prod_{p \leq \mathfrak{m}} p^{\frac{2}{p^2-1}(1-\frac{1}{p^{\mathfrak{n}(k,p)}})}\right) + \left(k + \frac{1}{2}\right)\log\left(1 - \frac{g_1}{k}\right)}{\log(k-g_1) - 1 + \log z_1} + \frac{(0.5\ell + 1)\log k - \log\left(\mathfrak{n}_1^{-1}\prod_{p\leq \mathfrak{m}} p^{1.5\mathfrak{n}(k,p)}\right)}{\log(k-g_1) - 1 + \log z_1} \tag{5.3}$$

and

$$g_1 > \frac{k \log\left(\frac{z_1 \mathfrak{n}_0}{2.71851} \prod_{p \leq \mathfrak{m}} p^{2/(p^2-1)}\right) + \left(k + \frac{1}{2}\right)\log\left(1 - \frac{g_1}{k}\right)}{\log(k-g_1) - 1 + \log z_1} - \frac{(1.5\pi(\mathfrak{m}) - 0.5\ell - 1)\log k + \log\left(\mathfrak{n}_1^{-1}\mathfrak{n}_2\prod_{p\leq \mathfrak{m}} p^{0.5+\frac{2}{p^2-1}}\right)}{\log(k-g_1) - 1 + \log z_1} \tag{5.4}$$

where

$$\mathfrak{n}(k,p)=\begin{cases}\left[\dfrac{\log(k-1)}{\log p}\right] & \textit{if } \left[\dfrac{\log(k-1)}{\log p}\right] \textit{ is even},\\ \left[\dfrac{\log(k-1)}{\log p}\right]-1 & \textit{if } \left[\dfrac{\log(k-1)}{\log p}\right] \textit{ is odd},\end{cases}\qquad \ell=|\{p\le\mathfrak{m}:p\,|\,d\}|,$$

$$\mathfrak{n}_0=\prod_{\substack{p|d\\ p\le\mathfrak{m}}}p^{\frac{1}{p+1}},\qquad \mathfrak{n}_1=\prod_{\substack{p|d\\ p\le\mathfrak{m}}}p^{\frac{p-1}{2(p+1)}},\qquad \mathfrak{n}_2=\begin{cases}2^{1/6} & \textit{if } 2\nmid d,\\ 1 & \textit{otherwise.}\end{cases}$$

Proof. Since $|R|\ge t-g+1=k-g_1+i_0$, we get

$$\prod_{b_i\in R}b_i\ge z_1^{k-g_1}(k-g_1)!. \tag{5.5}$$

Let

$$\vartheta_p=\operatorname{ord}_p\Big(\prod_{b_i\in R}b_i\Big),\qquad \vartheta'_p=1+\operatorname{ord}_p((k-1)!).$$

Let h be the positive integer such that $p^h\le k-1<p^{h+1}$, and $\varepsilon=1$ or 0 according as h is even or odd, respectively. Then

$$\vartheta'_p-1=\left[\frac{k-1}{p}\right]+\left[\frac{k-1}{p^2}\right]+\cdots+\left[\frac{k-1}{p^h}\right]. \tag{5.6}$$

Let $p\nmid d$. We show that

$$\vartheta_p-\vartheta'_p<-\frac{2k}{p^2-1}\left(1-\frac{1}{p^{\mathfrak{n}(k,p)}}\right)+1.5\mathfrak{n}(k,p) \tag{5.7}$$

$$<-\frac{2k}{p^2-1}+\frac{1.5\log k}{\log p}+0.5+\frac{2}{p^2-1}+\mathfrak{n}_3 \tag{5.8}$$

where $\mathfrak{n}_3=1/6$ if $p=2$ and 0 otherwise. We see that ϑ_p is the number of elements in $\{n+\gamma_1 d,n+\gamma_2 d,\dots,n+\gamma_t d\}$ divisible by p to an odd power. For a positive integer s with $s\le h$, let $0\le i_{p^s}<p^s$ be such that $p^s\,|\,(n+i_{p^s}d)$. Then we observe that p^s divides exactly $1+[(k-1-i_{p^s})/p^s]$ elements in $\{n,n+d,\dots,n+(k-1)d\}$. After removing a term in which p appears to a maximal power, the number of remaining elements in $\{n,n+d,\dots,$ $n+(k-1)d\}$ divisible by p to an odd power is at most

$$\left[\frac{k-1-i_p}{p}\right]-\left[\frac{k-1-i_{p^2}}{p^2}\right]+\left[\frac{k-1-i_{p^3}}{p^3}\right]-\cdots+(-1)^{\varepsilon}\left[\frac{k-1-i_{p^h}}{p^h}\right].$$

Since

$$\left[\frac{k}{p^s}\right]-1\le\left[\frac{k-1-i_{p^s}}{p^s}\right]\le\left[\frac{k-1}{p^s}\right],$$

we obtain

$$\vartheta_p - 1 \leq \left[\frac{k-1}{p}\right] - \left[\frac{k}{p^2}\right] + \left[\frac{k-1}{p^3}\right] - \cdots + (-1)^{\varepsilon}\left[\frac{k-1+\varepsilon}{p^h}\right] + \frac{h-1+\varepsilon}{2}.$$

This with (5.6) implies

$$\vartheta_p - \vartheta'_p \leq -\sum_{j=1}^{(h-1+\varepsilon)/2}\left(\left[\frac{k-1}{p^{2j}}\right] + \left[\frac{k}{p^{2j}}\right]\right) + \frac{h-1+\varepsilon}{2}. \tag{5.9}$$

Since $\left[\frac{k}{p^{2j}}\right] \geq \left[\frac{k-1}{p^{2j}}\right] \geq \frac{k-1}{p^{2j}} - 1 + \frac{1}{p^{2j}} = \frac{k}{p^{2j}} - 1$, we obtain

$$\vartheta_p - \vartheta'_p \leq -2k\sum_{j=1}^{(h-1+\varepsilon)/2}\frac{1}{p^2} + 1.5(h-1+\varepsilon),$$

giving (5.7) since $\mathfrak{n}(k,p) = h-1+\varepsilon$. Further, from (5.7), $k \leq p^{h+1}$ and $h < \log k/\log p$, we get

$$\vartheta_p - \vartheta'_p < -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p} + \frac{2p^{2-\varepsilon}}{p^2-1} + 1.5(\varepsilon - 1),$$

proving (5.8). For $p \mid d$, we get $\vartheta_p - \vartheta'_p = -1 - \mathrm{ord}_p(k-1)!$, which together with Lemma 5.1(v) gives

$$\begin{aligned}\vartheta_p - \vartheta'_p &< -\frac{k}{p-1} + \frac{\log k}{\log p} + \frac{1}{p-1}\\ &< -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p}\\ &\quad + 0.5 + \frac{2}{p^2-1} - \frac{k}{p+1} - \frac{0.5\log k}{\log p} - \frac{p-1}{2(p+1)}.\end{aligned} \tag{5.10}$$

For $\mathfrak{m} > 1$, we have

$$\prod_{b_i \in R} b_i \mid (k-1)!\Big(\prod_{p\leq k} p\Big)\prod_{p\leq \mathfrak{m}} p^{\vartheta_p - \vartheta'_p}.$$

Therefore from Lemma 5.1(iii), (5.10), (5.7) and (5.8), we have

$$\begin{aligned}\prod_{b_i\in R} b_i &< k!k^{-0.5\ell-1}\Big(\mathfrak{n}_1^{-1}\prod_{p\leq\mathfrak{m}} p^{1.5\mathfrak{n}(k,p)}\Big)\\ &\quad\times\left(\frac{\mathfrak{n}_0}{2.71851}\prod_{p\leq\mathfrak{m}} p^{\frac{2}{p^2-1}\left(1-\frac{1}{p^{\mathfrak{n}(k,p)}}\right)}\right)^{-k}\end{aligned} \tag{5.11}$$

and

$$\prod_{b_i\in R} b_i < k!k^{1.5\pi(\mathfrak{m})-0.5\ell-1}\Big(\mathfrak{n}_1^{-1}\mathfrak{n}_2\prod_{p\le\mathfrak{m}} p^{0.5+\frac{2}{p^2-1}}\Big) \times\left(\frac{\mathfrak{n}_0}{2.71851}\prod_{p\le\mathfrak{m}} p^{2/(p^2-1)}\right)^{-k}. \tag{5.12}$$

Comparing (5.11) and (5.12) with (5.5), we get

$$\frac{z_1^{g_1}k!}{(k-g_1)!} > k^{0.5\ell+1}\Big(\mathfrak{n}_1^{-1}\prod_{p\le\mathfrak{m}} p^{1.5\mathfrak{n}(k,p)}\Big)^{-1} \times\left(\frac{z_1\mathfrak{n}_0}{2.71851}\prod_{p\le\mathfrak{m}} p^{\frac{2}{p^2-1}(1-\frac{1}{p^{\mathfrak{n}(k,p)}})}\right)^{k} \tag{5.13}$$

and

$$\frac{z_1^{g_1}k!}{(k-g_1)!} > k^{-1.5\pi(\mathfrak{m})+0.5\ell+1}\Big(\mathfrak{n}_1^{-1}\mathfrak{n}_2\prod_{p\le\mathfrak{m}} p^{0.5+\frac{2}{p^2-1}}\Big)^{-1} \times\left(\frac{z_1\mathfrak{n}_0}{2.71851}\prod_{p\le\mathfrak{m}} p^{2/(p^2-1)}\right)^{k}. \tag{5.14}$$

By Lemma 5.2, we have

$$\frac{z_1^{g_1}k!}{(k-g_1)!} < z_1^{g_1}e^{-g_1}(k-g_1)^{g_1}\left(\frac{k}{k-g_1}\right)^{k+1/2} = \left(\frac{z_1(k-g_1)}{e}\right)^{g_1}\left(1-\frac{g_1}{k}\right)^{-k-1/2}.$$

This together with (5.13) and (5.14) implies the assertions (5.3) and (5.4), respectively. ∎

Inequality (5.8) corrects the corresponding inequality in [Lai06, p. 466, line 3 from the bottom] used in [Lai06, Lemma 13] but the proof of [Lai06, Lemma 13] remains unaffected.

We end this section with a lemma which follows immediately from [Lai06, Lemma 10].

LEMMA 5.5. *Let $t = k$. Let $c > 0$ be such that $c2^{\omega(d)-3} > 248$, $\mu \ge 2$ and*

$$\mathfrak{C}_\mu = \left\{A_i : i\in T_1,\ \nu(A_i)=\mu,\ A_i > \frac{\varrho 2^\delta k}{3c2^{\omega(d)}}\right\}.$$

Then

$$\mathfrak{C} := \sum_{\mu\ge 2}\frac{\mu(\mu-1)}{2}\,|\mathfrak{C}_\mu| \le \frac{3c}{32}\,4^{\omega(d)}(\log c2^{\omega(d)-3}). \tag{5.15}$$

6. Some counting functions. Let p be a prime $\leq k$ and coprime to d. Then the number of i's for which b_i are divisible by q is at most

$$\sigma_q = \lceil k/q \rceil.$$

Let $r \geq 5$ be any positive integer. Define $F(k, r)$ and $F'(k, r)$ as

$$F(k, r) = |\{i : P(b_i) > p_r\}| \quad \text{and} \quad F'(k, r) = \sum_{i=r+1}^{\pi(k)} \sigma_{p_i}.$$

Then

$$|\{b_i : P(b_i) > p_r\}| \leq F(k, r) \leq F'(k, r) - \sum_{p|d,\, p>p_r} \sigma_p.$$

Let

$$\mathcal{B}_r = \{b_i : P(b_i) \leq p_r\}, \qquad I_r = \{i : b_i \in \mathcal{B}_r\}, \qquad \xi_r = |I_r|.$$

We have

$$\xi_r \geq t - F(k, r) \geq t - F'(k, r) + \sum_{p|d,\, p>p_r} \sigma_p \tag{6.1}$$

and

$$t - |R| \geq t - |\{b_i : P(b_i) > p_r\}| - |\{b_i : P(b_i) \leq p_r\}| \tag{6.2}$$

$$\geq t - F(k, r) - |\{b_i : P(b_i) \leq p_r\}| \tag{6.3}$$

$$\geq t - F'(k, r) + \sum_{p|d,\, p>p_r} \sigma_p - |\{b_i : P(b_i) \leq p_r\}| \tag{6.4}$$

$$\geq t - F'(k, r) + \sum_{p|d,\, p>p_r} \sigma_p - 2^r. \tag{6.5}$$

We write $\mathcal{S} := \mathcal{S}(r)$ for the set of positive squarefree integers composed of primes $\leq p_r$. Let $\delta = \min\{3, \operatorname{ord}_2(d)\}$. Let $p = q = 2^\delta$, or let $p \leq q$ be odd primes dividing d. Let $p = q = 2^\delta$. Then $b_i \equiv n \pmod{2^\delta}$. Considering elements of $\mathcal{S}(r)$ modulo 2^δ, we see by induction on r that

$$|\{b_i : P(b_i) \leq p_r\}| \leq 2^{r-\delta} =: g_{2^\delta, 2^\delta} =: g_{2^\delta}. \tag{6.6}$$

For any odd prime p dividing d, all b_i's are either quadratic residues mod p or non-quadratic residues mod p. For odd primes p, q dividing d with $p \leq q$, we consider four sets:

$$(6.7)\quad \begin{aligned} \mathcal{S}_1(n',r) &= \mathcal{S}_1(\delta,n',p,q,r)\\ &= \left\{s\in\mathcal{S} : s\equiv n' \ (\mathrm{mod}\, 2^\delta), \left(\frac{s}{p}\right)=1, \left(\frac{s}{q}\right)=1\right\},\\ \mathcal{S}_2(n',r) &= \mathcal{S}_2(\delta,n',p,q,r)\\ &= \left\{s\in\mathcal{S} : s\equiv n' \ (\mathrm{mod}\, 2^\delta), \left(\frac{s}{p}\right)=1, \left(\frac{s}{q}\right)=-1\right\},\\ \mathcal{S}_3(n',r) &= \mathcal{S}_3(\delta,n',p,q,r)\\ &= \left\{s\in\mathcal{S} : s\equiv n' \ (\mathrm{mod}\, 2^\delta), \left(\frac{s}{p}\right)=-1, \left(\frac{s}{q}\right)=1\right\},\\ \mathcal{S}_4(n',r) &= \mathcal{S}_4(\delta,n',p,q,r)\\ &= \left\{s\in\mathcal{S} : s\equiv n' \ (\mathrm{mod}\, 2^\delta), \left(\frac{s}{p}\right)=-1, \left(\frac{s}{q}\right)=-1\right\}. \end{aligned}$$

We take $n'=1$ if $\delta=0,1$; $n'=1,3$ if $\delta=2$; and $n'=1,3,5,7$ if $\delta=3$. Let

$$(6.8)\qquad g_{p,q} := g_{p,q}(r) = \max_{n'}(|\mathcal{S}_1(n',r)|, |\mathcal{S}_2(n',r)|, |\mathcal{S}_3(n',r)|, |\mathcal{S}_4(n',r)|)$$

and write $g_p = g_{p,p}$. Then

$$(6.9)\qquad |\{b_i : P(b_i)\le p_r\}| \le g_{p,q}.$$

In view of (6.6) and (6.9), inequality (6.4) is improved as

$$(6.10)\qquad t-|R| \ge t - F'(k,r) + \sum_{p|d,\, p>p_r} \sigma_p - \min_{p|d,\, q|d}\{g_{p,q}\}.$$

We observe that $\gcd(s,pq)=1$ for $s\in\mathcal{S}_l$, $1\le l\le 4$. Hence we see that $\mathcal{S}_l(n',r+1)=\mathcal{S}_l(n',r)$ if $p=p_{r+1}$ or $q=p_{r+1}$, implying

$$(6.11)\qquad g_{p,q}(r+1) = g_{p,q}(r) \quad \text{if } p=p_{r+1} \text{ or } q=p_{r+1}.$$

Assume that $p_{r+1}\notin\{p,q\}$. Let $1\le l\le 4$. We write $\mathcal{S}'_l(n',r+1)=\{s : s\in\mathcal{S}_l(n',r+1),\ p_{r+1}\,|\,s\}$. Then $s=p_{r+1}s'$ with $P(s')\le p_r$ whenever $s\in\mathcal{S}'_l(n',r+1)$. Let $l=1$. Then $s'\equiv n'p_{r+1}^{-1}\equiv n'' \ (\mathrm{mod}\, 2^\delta)$ where $n''=1$ if $\delta=0,1$; $n''=1,3$ if $\delta=2$; and $n''=1,3,5,7$ if $\delta=3$. Further, $\left(\frac{s'}{p}\right)=\left(\frac{p_{r+1}}{p}\right)$ and $\left(\frac{s'}{q}\right)=\left(\frac{p_{r+1}}{q}\right)$ for $s\in\mathcal{S}'_l(r+1)$. This implies $\mathcal{S}'_1(n',r+1)=p_{r+1}\mathcal{S}_m(n'',r)$ for some m, $1\le m\le 4$. Therefore $|\mathcal{S}'_1(n',r+1)|\le g_{p,q}(r)$ by (6.8). Similarly $|\mathcal{S}'_l(n',r+1)|\le g_{p,q}(r)$ for each l, $1\le l\le 4$. Hence we see from $\mathcal{S}_l(n',r+1)=\mathcal{S}_l(n',r)\cup\mathcal{S}'_l(n',r+1)$ that

$$(6.12)\qquad g_{p,q}(r+1)\le 2g_{p,q}(r).$$

We now use the above assertions to calculate $g_{p,q}$.

(i) Let $5 \le r \le 7$, $p \le 547$ when $\delta = 0, 1$; $5 \le r \le 7$, $p \le 547$ when $\delta = 2$; and $5 \le r \le 7$, $p \le 89$ when $\delta = 3$. Then

$$g_p(r) = \begin{cases} \max(1, 2^{r-\delta-2}) & \text{if } p \le p_r, \\ \max(1, 2^{r-\delta-1}) & \text{if } p > p_r, \end{cases} \tag{6.13}$$

except when

- $\delta = 0$, $r = 5$, $p = 479$, where $g_p = 2^r$;
- $\delta = 1$, $r = 5$, $p \in \{131, 421, 479\}$ or $r = 6, p = 131$, where $g_p = 2^{r-\delta}$;
- $\delta = 2$, $r = 5$, $p \in \{41, 101, 131, 331, 379, 421, 461, 479, 499\}$, where $g_p = 2^{r-\delta}$;
- $\delta = 2$, $r = 6$, $p \in \{101, 131\}$ or $r = 7$, $p = 101$, where $g_p = 2^{r-\delta}$;
- $\delta = 3$, $r = 5$, $p = 3$, where $g_p = 2^{r-\delta-1}$, or $r = 5$, $p = 41$, where $g_p = 2^{r-\delta}$.

(ii) Let $5 \le r \le 7$, $p \le 19$, $q \le 193$, $23 \le p < q \le 97$ when $\delta = 0$, and $r = 5, 6$, $p < q \le 37$ when $\delta \ge 1$. Then

$$g_{p,q}(r) = \begin{cases} \max(1, 2^{r-\delta-4}) & \text{if } p < q \le p_r, \\ \max(1, 2^{r-\delta-3}) & \text{if } p \le p_r < q, \\ \max(1, 2^{r-\delta-2}) & \text{if } p_r < p < q, \end{cases} \tag{6.14}$$

except when

$$\delta = 0 \text{ and } \begin{cases} r = 5, \ g_{p,q} = 2^{r-2} \text{ for } (p,q) \in \{(5,43), (5,167), (7,113), \\ \qquad (7,127), (7,137), (11,61), (11,179), (11,181)\}; \\ r = 5, \ g_{p,q} = 2^{r-1} \text{ for } (p,q) \in \{(19,139), (23,73), (37,83)\}; \\ r = 6, \ g_{p,q} = 2^{r-2} \text{ for } (p,q) = (7,137); \\ r = 6, \ g_{p,q} = 2^{r-1} \text{ for } (p,q) = (37,83); \end{cases}$$

$$\delta = 1 \text{ and } \begin{cases} r = 5, \ g_{p,q} = 2^{r-4} \text{ for } (p,q) \in \{(5,7), (5,11)\}; \\ r = 5, \ g_{p,q} = 2^{r-3} \text{ for } (p,q) = (5,37); \\ r = 5, \ g_{p,q} = 2^{r-2} \text{ for } (p,q) \in \{(13,23), (29,31)\}; \\ r = 6, \ g_{p,q} = 2^{r-4} \text{ for } (p,q) = (5,7); \end{cases}$$

$$\delta = 2 \text{ and } \begin{cases} r = 5, \ g_{p,q} = 2^{r-4} \text{ for } (p,q) \in \{(3,19), (5,17), (5,37), (7,13), \\ \qquad (7,23), (7,29), (7,31), (11,19), (11,29), (11,31)\}; \\ r = 5, \ g_{p,q} = 2^{r-3} \text{ for } (p,q) \in \{(13,23), (17,37), (29,31)\}; \\ r = 6, \ g_{p,q} = 2^{r-5} \text{ for } (p,q) \in \{(5,7), (7,13)\}; \\ r = 6, \ g_{p,q} = 2^{r-4} \text{ for } (p,q) \in \{(7,29), (11,31), (13,23)\}. \end{cases}$$

Now we combine (6.13), (6.14), (6.12) and (6.11). We obtain (6.13) with $=$ replaced by $\le$ for $r \ge 7$ and $p \le 89$, and we shall refer to it as (6.13, $\le$). Further, we obtain (6.14) with $=$ replaced by $\le$ for $r \ge 7$ and either $p < q \le 97$ when $\delta = 0$, or $p = 3$, $q = 5$ when $\delta \ge 1$, and we shall refer to it as (6.14, $\le$).

7. Computational lemmas. From now on, we take $t=k$. Thus $b_j = a_{j-1}$, $B_j = A_{j-1}$, $y_j = x_{j-1}$ and $Y_j = X_{j-1}$ for $1 \le j \le k$. Let $\bar{f}(x) = \lceil x \rceil - [\lceil x \rceil/4]$ for $x > 0$ and $\mathcal{K}_a = k/a2^{3-\delta}$ for $a \in R$. We now state a result which generalises [HLST07, Lemma 1].

LEMMA 7.1. *Let* $a \in R$ *and* μ *be a positive integer. Let* p, q *be distinct odd primes.*

(i) *Let*

$$f_0(k,a,\delta) = \bar{f}(\mathcal{K}_a),$$

$$f_1(k,a,p,\mu,\delta) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\bar{f}\left(\frac{\mathcal{K}_a}{p^{2l+1}}\right) + \bar{f}\left(\frac{\mathcal{K}_a}{p^{2\mu}}\right),$$

$$f_2(k,a,p,q,\mu,\delta) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\left(\frac{q-1}{2}\,\bar{f}\left(\frac{\mathcal{K}_a}{p^{2l+1}q}\right)+\bar{f}\left(\frac{\mathcal{K}_a}{p^{2l+1}q^2}\right)\right)+\bar{f}\left(\frac{\mathcal{K}_a}{p^{2\mu}}\right).$$

Then

$$\nu_{\mathrm{o}}(a) \le \begin{cases} f_0(k,a,\delta), & \\ f_1(k,a,p,\mu,\delta) & \text{if } p\nmid d, \\ f_2(k,a,p,q,\mu,\delta) & \text{if } p\nmid d,\ q\nmid d. \end{cases} \tag{7.1}$$

(ii) *Let* d *be odd. Let*

$$g_0(k,a,\mu) = \sum_{l=1}^{\mu-1}\bar{f}\left(\frac{\mathcal{K}_a}{2^{2l}}\right) + \bar{f}\left(\frac{k}{a2^{2\mu}}\right),$$

$$g_1(k,a,p,\mu) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\sum_{j=1}^{2}\bar{f}\left(\frac{\mathcal{K}_a}{2^j p^{2l+1}}\right) + \sum_{j=1}^{2}\bar{f}\left(\frac{\mathcal{K}_a}{2^j p^{2\mu}}\right),$$

$$g_2(k,a,p,q,\mu) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\sum_{j=1}^{2}\left(\frac{q-1}{2}\,\bar{f}\left(\frac{\mathcal{K}_a}{2^j p^{2l+1}q}\right) + \bar{f}\left(\frac{\mathcal{K}_a}{2^j p^{2l+1}q^2}\right)\right)$$
$$+\sum_{j=1}^{2}\bar{f}\left(\frac{\mathcal{K}_a}{2^j p^{2\mu}}\right).$$

Then

$$\nu_{\mathrm{e}}(a) \le \begin{cases} g_0(k,a,\mu), & \\ g_1(k,a,p,\mu) & \text{if } p\nmid d, \\ g_2(k,a,p,q,\mu) & \text{if } p\nmid d,\ q\nmid d. \end{cases} \tag{7.2}$$

Proof. Let $\mathcal{I} \subseteq \{i : a_i = a\}$ and $\tau \mid (i-j)$ whenever $i, j \in \mathcal{I}$. Let τ' be the lcm of all τ_1 such that $\tau_1 \mid (i-j)$ whenever $i, j \in \mathcal{I}$. Then $\tau \mid \tau'$ and $a \mid \tau'$ since $a \mid (i-j)$ whenever $i, j \in \mathcal{I}$. Let $i_0 = \min_{i\in\mathcal{I}} i$, $N = (n+i_0 d)/a$ and $D = (\tau'/a)d$. Then we see that ax_i^2 with $i \in \mathcal{I}$ come from the squares in the set $\{N, N+D, \dots, N+(\lceil (k-i_0)/\tau\rceil - 1)D\}$. Dividing this set into consecutive intervals of length 4 and using Euler's result, we see that there are at most

$$\left\lceil \frac{k-i_0}{\tau'} \right\rceil - \left[\frac{\lceil \frac{k-i_0}{\tau'} \rceil}{4} \right] \le \left\lceil \frac{k}{\tau'} \right\rceil - \left[\frac{\lceil \frac{k}{\tau'} \rceil}{4} \right] = \bar{f}\left(\frac{k}{\tau'}\right)$$

of them which can be squares. Hence $|\mathcal{I}| \le \bar{f}(k/\tau') \le \bar{f}(k/\tau)$ since $\tau \mid \tau'$.

Let $\mathcal{I}^{\mathrm{o}} = \{i : a_i = a,\, 2 \nmid x_i\}$ and $\mathcal{I}^{\mathrm{e}} = \{i : a_i = a,\, 2 \mid x_i\}$. Then $\nu_{\mathrm{o}}(a) = |\mathcal{I}^{\mathrm{o}}|$ and $\nu_{\mathrm{e}}(a) = |\mathcal{I}^{\mathrm{e}}|$.

First we prove (7.1). For $i, j \in \mathcal{I}^{\mathrm{o}}$, we observe from $x_i^2, x_j^2 \equiv 1 \pmod 8$ and $(i-j)d = a(x_i^2 - x_j^2)$ that $a2^{3-\delta} \mid (i-j)$. Therefore $|\mathcal{I}^{\mathrm{o}}| \le \bar{f}(\mathcal{K}_a) = f_0(k, a, \delta)$.

For a prime p', let

$$\mathfrak{Q}_{p'} = \left\{ m : 1 \le m < p',\, \left(\frac{m}{p'}\right) = 1 \right\}.$$

Let $p \nmid d$. Let

$$\mathcal{I}^{\mathrm{o}}_l = \{i \in \mathcal{I}^{\mathrm{o}} : p^l \,\|\, x_i\} \quad \text{for } 0 \le l < \mu, \quad \mathcal{I}^{\mathrm{o}}_\mu = \{i \in \mathcal{I}^{\mathrm{o}} : p^\mu \mid x_i\}.$$

Then $a2^{3-\delta}p^{2\mu} \mid (i-j)$ whenever $i, j \in \mathcal{I}^{\mathrm{o}}_\mu$, giving $|\mathcal{I}^{\mathrm{o}}_\mu| \le \bar{f}(\mathcal{K}_a/p^{2\mu})$. For each l, $0 \le l < \mu$, and for each $m \in \mathfrak{Q}_p$, let

$$\mathcal{I}^{\mathrm{o}}_{lm} = \{i \in \mathcal{I}^{\mathrm{o}}_l : (x_i/p^l)^2 \equiv m \pmod p\}.$$

Then $a2^{3-\delta}p^{2l+1} | (i-j)$ whenever $i, j \in \mathcal{I}^{\mathrm{o}}_{lm}$, giving $|\mathcal{I}^{\mathrm{o}}_{lm}| \le \bar{f}(\mathcal{K}_a/p^{2l+1})$. Therefore

$$|\mathcal{I}^{\mathrm{o}}_l| = \sum_{m \in \mathfrak{Q}_p} |\mathcal{I}^{\mathrm{o}}_{lm}| \le \frac{p-1}{2}\, \bar{f}\left(\frac{\mathcal{K}_a}{p^{2l+1}}\right).$$

Hence $|\mathcal{I}^{\mathrm{o}}| = |\mathcal{I}^{\mathrm{o}}_\mu| + \sum_{l=0}^{\mu-1} |\mathcal{I}^{\mathrm{o}}_l| \le f_1(k, a, p, \mu, \delta)$.

Thus we may assume that $p \nmid d$ and $q \nmid d$. For each l with $0 \le l < \mu$, $m \in \mathfrak{Q}_p$ and for each $u \in \mathfrak{Q}_q$, let

$$\mathcal{I}^{\mathrm{o}}_{lmu} = \{i \in \mathcal{I}^{\mathrm{o}}_{lm} : x_i^2 \equiv u \pmod q\}, \quad \mathcal{I}^{\mathrm{o}}_{lm0} = \{i \in \mathcal{I}^{\mathrm{o}}_{lm} : q \mid x_i\}.$$

Then $a2^{3-\delta}p^{2l+1}q \mid (i-j)$ for $i, j \in \mathcal{I}^{\mathrm{o}}_{lmu}$ and $a2^{3-\delta}p^{2l+1}q^2 \mid (i-j)$ for $i, j \in \mathcal{I}^{\mathrm{o}}_{lm0}$, implying $|\mathcal{I}^{\mathrm{o}}_{lmu}| \le \bar{f}(\mathcal{K}_a/p^{2l+1}q)$ for $u \in \mathfrak{Q}_q$ and $|\mathcal{I}^{\mathrm{o}}_{lm0}| \le \bar{f}(\mathcal{K}_a/p^{2l+1}q^2)$. Now the assertion $\nu_{\mathrm{o}}(a) \le f_2(k, a, p, q, \mu, \delta)$ follows from

$$|\mathcal{I}^{\mathrm{o}}_{lm}| \le |\mathcal{I}^{\mathrm{o}}_{lm0}| + \sum_{u \in \mathfrak{Q}_q} |\mathcal{I}^{\mathrm{o}}_{lmu}|, \quad |\mathcal{I}^{\mathrm{o}}_l| = \sum_{m \in \mathfrak{Q}_p} |\mathcal{I}^{\mathrm{o}}_{lm}|, \quad |\mathcal{I}^{\mathrm{o}}| = |\mathcal{I}^{\mathrm{o}}_\mu| + \sum_{l=0}^{\mu-1} |\mathcal{I}^{\mathrm{o}}_l|.$$

Now we turn to the proof of (7.2). Let

$$\mathcal{I}^{\mathrm{e}l} = \{i \in \mathcal{I}^{\mathrm{e}} : 2^l \,\|\, x_i\} \quad \text{for } 1 \le l < \mu \quad \text{and} \quad \mathcal{I}^{\mathrm{e}\mu} = \{i \in \mathcal{I}^{\mathrm{e}} : 2^\mu \mid x_i\}.$$

Since $x_i/2^l$ is odd, we get $a2^{2l+3} | (i-j)$ whenever $i, j \in \mathcal{I}^{\mathrm{e}l}$, implying $|\mathcal{I}^{\mathrm{e}l}| \le \bar{f}(\mathcal{K}_a/2^{2l})$ for $0 \le l < \mu$. Further, $a2^{2\mu} \mid (i-j)$ for $i, j \in \mathcal{I}^{\mathrm{e}\mu}$, giving $|\mathcal{I}^{\mathrm{e}\mu}|$

$\le \bar{f}(k/a2^{2\mu})$. Now the assertion $\nu_{\mathrm{e}}(a) \le g_0(k,a,\mu)$ follows from $|\mathcal{I}^{\mathrm{e}}| = |\mathcal{I}^{\mathrm{e}\mu}| + \sum_{l<\mu} |\mathcal{I}^{\mathrm{e}l}|$.

For the remaining parts of (7.2), we consider $\mathcal{I}^{\mathrm{e}1} = \{i \in \mathcal{I}^{\mathrm{e}} : 2 \parallel x_i\}$, $\mathcal{I}^{\mathrm{e}2} = \{i \in \mathcal{I}^{\mathrm{e}} : 4 \mid x_i\}$ so that $|\mathcal{I}^{\mathrm{e}}| = |\mathcal{I}^{\mathrm{e}1}| + |\mathcal{I}^{\mathrm{e}2}|$. Then $32a \mid (i-j)$ for $i,j \in \mathcal{I}^{\mathrm{e}1}$ and $16a \mid (i-j)$ for $i,j \in \mathcal{I}^{\mathrm{e}2}$. We now continue the proof as in that of (7.1) with $\mathcal{I}^{\mathrm{e}1}, \mathcal{I}^{\mathrm{e}2}$ in place of $\mathcal{I}^{\mathrm{o}}$ to get $\nu_{\mathrm{e}}(a) \le g_1(k,a,p,\mu)$ when $p \nmid d$ and $\nu_{\mathrm{e}}(a) \le g_2(k,a,p,q,\mu)$ when $p \nmid d,\ q \nmid d$. ■

LEMMA 7.2. *For* $a \in R$, *let*

$$f_3(k,a,\delta) = \begin{cases} 1 & \text{if } k \le a2^{3-\delta}, \\ \bar{f}(\mathcal{K}_a) & \text{if } k > a2^{3-\delta},\ 3 \mid d, 5 \mid d, \\ \bar{f}(\mathcal{K}_a/3) + \bar{f}(\mathcal{K}_a/9) & \text{if } k > a2^{3-\delta},\ 3 \nmid d,\ 5 \mid d, \\ \bar{f}(\mathcal{K}_a) & \text{if } a2^{3-\delta} < k \le 2a2^{3-\delta},\ 3 \mid d,\ 5 \nmid d, \\ 2\bar{f}(\mathcal{K}_a/5) + \bar{f}(\mathcal{K}_a/25) & \text{if } k > 2a2^{3-\delta},\ 3 \mid d,\ 5 \nmid d, \\ \bar{f}(\mathcal{K}_a/3) + \bar{f}(\mathcal{K}_a/9) & \text{if } a2^{3-\delta} < k \le 24a2^{3-\delta},\ 3 \nmid d,\ 5 \nmid d, \\ 2(\bar{f}(\mathcal{K}_a/15) + \bar{f}(\mathcal{K}_a/135)) & \\ \quad + \bar{f}(\mathcal{K}_a/75) + \bar{f}(\mathcal{K}_a/675) + \bar{f}(\mathcal{K}_a/81) & \\ & \text{if } 24a2^{3-\delta} < k \le 324a2^{3-\delta},\ 3 \nmid d,\ 5 \nmid d, \\ 2(\bar{f}(\mathcal{K}_a/15) + \bar{f}(\mathcal{K}_a/135) + \bar{f}(\mathcal{K}_a/1215)) & \\ \quad + \bar{f}(\mathcal{K}_a/75) + \bar{f}(\mathcal{K}_a/675) + \bar{f}(\mathcal{K}_a/6075) + \bar{f}(\mathcal{K}_a/729) & \\ & \text{if } k > 324a2^{3-\delta},\ 3 \nmid d,\ 5 \nmid d \end{cases}$$

and

$$g_3(k,a) = \begin{cases} 1 & \text{if } k \le 4a, \\ \sum_{j=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j}\right) & \text{if } 4a < k \le 32a, \\ \sum_{j=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j}\right) & \text{if } k > 32a,\ 3 \mid d,\ 5 \mid d, \\ \sum_{j=1}^{2} \left(\bar{f}\left(\frac{\mathcal{K}_a}{2\cdot 3^j}\right) + \bar{f}\left(\frac{\mathcal{K}_a}{4\cdot 3^j}\right)\right) & \text{if } k > 32a,\ 3 \nmid d,\ 5 \mid d, \end{cases}$$

$$g_3(k,a) = \begin{cases} \sum_{j=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j}\right) & \textit{if } 32a < k \le 64a,\ 3\,|\,d,\ 5\nmid d, \\ 2\sum_{j=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j\cdot 5}\right) + \sum_{j=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j\cdot 25}\right) & \textit{if } k > 64a,\ 3\,|\,d,\ 5\nmid d, \\ \sum_{j=1}^{2}\sum_{l=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j\cdot 3^l}\right) & \textit{if } 32a < k \le 576a,\ 3\nmid d,\ 5\nmid d, \\ 2\sum_{j=1}^{2}\sum_{l=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j\cdot 3^{2l-1}\cdot 5}\right) & \\ \quad + \sum_{j=1}^{2}\sum_{l=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j\cdot 3^{2l-1}\cdot 25}\right) + \sum_{j=1}^{2} \bar{f}\left(\frac{\mathcal{K}_a}{2^j\cdot 81}\right) & \\ & \textit{if } k > 576a,\ 3\nmid d,\ 5\nmid d. \end{cases}$$

Then for $a \in R$, we have

$$\nu_{\mathrm{o}}(a) \le f_3(k,a,\delta), \qquad \nu_{\mathrm{e}}(a) \le g_3(k,a)$$

and

$$\nu(a) \le F_0(k,a,\delta) := \begin{cases} 1 & \textit{if } k \le a, \\ f_3(k,a,\delta) & \textit{if } k > a \textit{ and } d \textit{ is even}, \\ f_3(k,a,0) + g_3(k,a) & \textit{if } k > a \textit{ and } d \textit{ is odd}. \end{cases}$$

Proof. Since $a\,|\,(i-j)$ whenever $a_i = a_j = a$, we get $\nu(a) \le 1$, $\nu_{\mathrm{o}}(a) \le 1$, $\nu_{\mathrm{e}}(a) \le 1$ for $k \le a$. In fact, $\nu_{\mathrm{o}}(a) \le 1$ for $k \le a2^{3-\delta}$ and $\nu_{\mathrm{e}}(a) \le 1$ for $k \le 4a$. Thus we suppose that $k > a$. We have $\nu(a) = \nu_{\mathrm{o}}(a) + \nu_{\mathrm{e}}(a)$. It suffices to show $\nu_{\mathrm{o}}(a) \le f_3(k,a,\delta)$ for $k > a2^{3-\delta}$ and $\nu_{\mathrm{e}}(a) \le g_3(k,a)$ for $k > 4a$ since $\nu_{\mathrm{e}}(a) = 0$ for d even. From (7.1), we get the assertion $\nu_{\mathrm{o}}(a) \le f_3(k,a,\delta)$ for $k > a2^{3-\delta}$ since

$$\nu_{\mathrm{o}}(a) \le \begin{cases} f_0(k,a,\delta) & \text{if } 15\,|\,d, \\ f_1(k,a,3,1,\delta) & \text{if } 3\nmid d,\ 5\,|\,d, \\ \min(f_0(k,a,\delta), f_1(k,a,5,1,\delta)) & \text{if } 3\,|\,d,\ 5\nmid d, \\ \min(f_1(k,a,3,1,\delta), f_2(k,a,3,5,2,\delta), & \\ \qquad\qquad f_2(k,a,3,5,3,\delta)) & \text{if } 3\nmid d,\ 5\nmid d. \end{cases}$$

The assertion $\nu_e(a) \le g_3(k,a)$ for $k > 4a$ follows from (7.2) since $\nu_e(a) \le g_0(k,a,2)$ for $4a < k \le 32a$ and

$$\nu_e(a) \le \begin{cases} g_0(k,a,2) & \text{if } 15 \mid d, \\ g_1(k,a,3,1) & \text{if } 3 \nmid d,\ 5 \mid d, \\ \min(g_0(k,a,2), g_1(k,a,5,1)) & \text{if } 3 \mid d,\ 5 \nmid d, \\ \min(g_1(k,a,3,1), g_2(k,a,3,5,2)) & \text{if } 3 \nmid d,\ 5 \nmid d \end{cases}$$

for $k > 32a$. ∎

By applying the fact that there are $(p-1)/2$ distinct quadratic residues and $(p-1)/2$ distinct quadratic non-residues modulo a prime p, we have

LEMMA 7.3. *Assume* (1.1) *holds with* $k \nmid d$. *Then* $\nu(a) \le (k-1)/2$ *for any* $a \in R$.

LEMMA 7.4. *Suppose that* (1.1) *with* $P(b) \le k$ *and* $k = p_m$ *has no solution. Then* (1.1) *with* $P(b) \le k$ *and* $p_m \le k < p_{m+1}$ *has no solution.*

Proof. Let $p_m \le k < p_{m+1}$. Suppose (n,d,b,y) is a solution of

$$n(n+d)\cdots(n+(k-1)d) = by^2$$

with $P(b) \le k$. Then $P(b) \le p_m$, and by (1.5),

$$n(n+d)\cdots(n+(p_m-1)d) = b'y'^2$$

for some b' with $P(b') \le p_m$, giving a solution of (1.1) at $k = p_m$. This is a contradiction. ∎

LEMMA 7.5. *Let* $k \ge 101$. *Assume* (1.1).

(a) *Let d be odd and $p < q$ be primes such that $pq \mid d$ with $p \le 19$, $q \le 47$. Then $k \ge 1733$.*
(b) *Let d be odd and $p < q$ be primes such that $pq \mid d$ with $23 \le p < q \le 43$, $(p,q) \ne (31,41)$. Then $k \ge 1087$.*
(c) *Let d be even such that $p \mid d$ with $3 \le p \le 47$. Then $k \ge 1801$.*

Proof. We shall use the notation and results of Section 6 without reference. By Lemma 7.4, it suffices to prove Lemma 7.5 when k is a prime. Let P_0 be the largest prime $\le k$ such that $P_0 \nmid d$. Then (1.1) holds at $k = P_0$. Therefore $P_0 \ge 101$ by Theorem $\mathcal{A}$ with $k = 97$. Thus there is no loss of generality in assuming that $k \nmid d$ for the proof of Lemma 7.5.

(a) Let d be odd and p, q be as in (a). Assume $k < 1733$. It suffices to consider four cases, viz. (i) $5 < p < q$, $3 \nmid d$, $5 \nmid d$; (ii) $p = 3$, $q > 5$, $5 \nmid d$; (iii) $p = 5$, $q > 5$, $3 \nmid d$, and (iv) $p = 3$, $q = 5$. We take $r \ge 7$. We see that $\mathcal{B}_r$ is contained in one of the four sets $\mathcal{S}_\mu = \mathcal{S}_\mu(1,r)$ with $1 \le \mu \le 4$. Let $\mathcal{S}'_\mu = \{s \in \mathcal{S}_\mu : s < 2000\}$ with $1 \le \mu \le 4$. We have $\nu(s) \le F_0(k,s,0)$ by Lemma 7.2. Further, $\nu(s) \le 1$ for $s \ge k$ and hence for $s \in \mathcal{S}_\mu \setminus \mathcal{S}'_\mu$. Observe that $1 \in \mathcal{S}'_1 \subseteq \mathcal{S}_1$.

Assume that $1 \notin R$ in case (iv). For case (i), we take $r = 7$ for $101 \le k < 1087$ and $r = 8$ for $1087 \le k < 1733$. For all other cases, we take $r = 7$ for $101 \le k < 941$, $r = 8$ for $941 \le k < 1297$ and $r = 9$ for $1297 \le k < 1733$. Then

$$\begin{aligned}\xi_r &\le \max \sum_{s\in\mathcal{S}_\mu} \nu(s) \le \max\Big(g_{p,q} - |\mathcal{S}'_\mu| + \sum_{s\in\mathcal{S}'_\mu} F(k,s,0)\Big)\\ &\le g_{p,q} + \max \sum_{s\in\mathcal{S}'_\mu} (F_0(k,s,0)-1) =: \widetilde{\xi}_r\end{aligned}$$

where the maximum is taken over $1 \le \mu \le 4$ and we remove 1 from $\mathcal{S}'_1 \subseteq \mathcal{S}_1$ when case (iv) holds. We now check that

$$k - F'(k,r) - \widetilde{\xi}_r > \begin{cases} 0 & \text{if } p < q \le \mathfrak{p}_r,\\ -\lceil k/q\rceil & \text{if } p \le \mathfrak{p}_r < q,\\ -\lceil k/p\rceil - \lceil k/q\rceil & \text{if } \mathfrak{p}_r < p < q.\end{cases} \tag{7.3}$$

This contradicts (6.1) by using the estimates for $g_{p,q}$ and $\widetilde{\xi}_r \ge \xi_r$.

Thus it remains to consider (iv) with $1 \in R$. Then $\left(\frac{a_i}{3}\right) = \left(\frac{a_i}{5}\right) = 1$ for all $a_i \in R$. Suppose that $p' \nmid d$ for some prime $p' \in \mathcal{P} = \{7, 11, 13\}$. We take $r = 9$. We have $\mathcal{B}_r \subseteq \mathcal{S}_1$. Further, $|\mathcal{S}_1| = 32$ and $\mathcal{S}'_1 = \{1, 19, 34, 46, 91, 154, 286, 391, 646, 874, 1309, 1729, 1771\}$. We deduce from (7.1) that

$$\begin{aligned}\nu_{\mathrm{o}}(a) &\le \min(f_0(k,a,0), f_1(k,a,p',1,0))\\ &\le \min(f_0(k,a,0), \max_{p'\in\mathcal{P}}\{f_1(k,a,p',1,0)\}) =: G_1(k,a).\end{aligned}$$

Similarly we infer from (7.2) that

$$\nu_{\mathrm{e}}(a) \le \min(g_0(k,a,2), \max_{p'\in\mathcal{P}}\{g_1(k,a,p',1,0)\}) =: G_2(k,a).$$

Let $G(k,a) = 1$ if $k \le a$ and $G(k,a) = G_1(k,a) + G_2(k,a)$ if $k > a$. Then $\nu(a) \le G(k,a)$ implying $\xi_r \le 32 + \sum_{s\in\mathcal{S}'_1}(G(k,s)-1) =: \widetilde{\xi}_r$ as above. We check that

$$k - F'(k,r) - \widetilde{\xi}_r > 0. \tag{7.4}$$

This contradicts (6.1). Thus $p' \mid d$ for each prime $p \in \mathcal{P}$. Now we take $r = 14$. Since $1 \in R$, we have $\left(\frac{a_i}{p}\right) = 1$ for all $a_i \in R$ and for each p with $3 \le p \le 13$. Therefore $\mathcal{B}_r \subseteq \left\{s \in \mathcal{S}(r) : \left(\frac{s}{p}\right) = 1, 3 \le p \le 13\right\} = \{1, 1054\} \cup \mathcal{S}''$ where $|\mathcal{S}''| = 14$ and $s > 2000$ for each $s \in \mathcal{S}''$. Hence $\xi_r \le \nu(1) + \nu(1054) + 14 \le \nu(1) + 16$ since $\nu(1054) \le 2$ by Lemma 7.2. From (7.1) and (7.2) with $\mu = 3$, we get $\nu(1) \le f_0(k,1,0) + g_0(k,1,3)$. Therefore $\xi_r \le f_0(k,1,0) + g_0(k,1,3) + 16 =: \widetilde{\xi}_r$ and we compute that (7.4) holds, contradicting (6.1).

(b) Let d be odd and p, q be as in (b). Assume $k < 1013$. By (a), we may assume that $3 \nmid d, 5 \nmid d$. We continue the proof as above in case (i) of (a).

We take $r=7$ and check that $k-F'(k,r)-\widetilde{\xi}_r+\lceil k/p\rceil+\lceil k/q\rceil>0$. This contradicts (6.1).

(c) Let d be even and p be as in (c). Assume $k<1801$. For any set W of squarefree integers, let $W'=W'(\delta)=\{s\in W : s<2000/2^{3-\delta}\}$. We consider four cases, viz. (i) $p>5,\ 3\nmid d,\ 5\nmid d$; (ii) $p=5,\ 3\nmid d$; (iii) $p=3,\ 5\nmid d$; and (iv) $15\,|\,d$. We take $r\geq 7$. Assume that (i), (ii) or (iii) holds. Then from (6.7) with $p=q$, we get 2^δ sets $U_\mu,\ 1\leq\mu\leq 2^\delta$, given by $\mathcal{S}_1(n',r),\mathcal{S}_4(n',r)$. Without loss of generality, we put $\mathcal{S}_1(1,r)=U_1$. Further, $|U_\mu|\leq g_p$ for $1\leq\mu\leq 2^\delta$. Assume (iv). We take $p=3,q=5$ in (6.7). We get $2^{\delta+1}$ sets $V_\mu, 1\leq\mu\leq 2^{\delta+1}$, given by $\mathcal{S}_j(n',r),\ 1\leq j\leq 4$, and we put $\mathcal{S}_1(1,r)=V_1$. Further, $|V_\mu|\leq 2^{r-\delta-4}$ for $1\leq\mu\leq 2^{\delta+1}$. We define g' by $g'=2^{r-\delta-4}$ if (iv) holds and $g'=g_p$ otherwise. Further, let W_μ with $1\leq\mu\leq 2^{\delta+1}$ be given by $W_\mu=V_\mu$ if (iv) holds, and $W_\mu=U_\mu$ for $1\leq\mu\leq 2^\delta$, $W_\mu=\emptyset$ for $\mu>2^\delta$ if (i), (ii) or (iii) holds. We see from Lemma 7.2 that $\nu(s)\leq F_0(k,s,\delta)$ and $\nu(s)\leq 1$ for $s\in W_\mu\setminus W'_\mu$. Observe that $1\in W'_1\subseteq W_1$.

Assume that $1\notin R$ in cases (ii), (iii) or (iv). We take $r=8$ for $101\leq k\leq 941$, $r=9$ for $941<k\leq 1373$ and $r=10$ for $1373<k<1801$ in case (i) with $8\,|\,d$. For all other cases, we take $r=7$ for $101\leq k\leq 941$, $r=8$ for $941<k\leq 1373$ and $r=9$ for $1373<k<1801$. Then $\xi_r\leq \max\sum_{s\in W_\mu}F(k,s,\delta)\leq g'+\max\sum_{s\in W'_\mu}(F_0(k,s,\delta)-1)=:\widetilde{\xi}_r$, where the maximum is taken over $1\leq\mu\leq 2^{\delta+1}$ and we remove 1 from $W'_1\subseteq W_1$ when (ii), (iii) or (iv) holds. We check that

$$k-F'(k,r)-\widetilde{\xi}_r>\begin{cases}-\lceil k/p\rceil & \text{if (i) holds with } p>p_r,\\ 0 & \text{otherwise.}\end{cases}$$

This contradicts (6.1).

Thus it remains to consider cases (ii), (iii) or (iv) and $1\in R$. Then $a_i\equiv 1 \pmod{2^\delta}$ and $\left(\frac{a_i}{p}\right)=1$ for all $p\,|\,d$ whenever $a_i\in R$. Let $P_0=\{5\},\{3\},\{3,5\}$ when (ii), (iii), (iv) holds, respectively. Then $\left(\frac{a_i}{p}\right)=1$ for $p\in P_0$.

Assume that $7\nmid d$ when $8\,|\,d,\ 15\,|\,d$. Let $\mathcal{P}=\{7\}$ if $8\,|\,d,\ 3\,|\,d,\ 5\nmid d$; $\mathcal{P}=\{7,11,13,17,19\}$ if $4\,\|\,d,\ 15\,|\,d$; $\mathcal{P}=\{11,13,17,19\}$ if $8\,|\,d,\ 15\,|\,d$; $\mathcal{P}=\{7,11,13\}$ in all other cases. Suppose that $p'\nmid d$ for some prime $p'\in\mathcal{P}$. Let r be given by the following table:

(ii), (iii), $2\,\|\,d,\ 4\,\|\,d$	(ii), (iii), $8\,|\,d$	(iv), $2\,\|\,d$	(iv), $4\,\|\,d,\ 8\,|\,d$
$\begin{cases}8 \text{ for } k\leq 941,\\ 9 \text{ for } k>941\end{cases}$	$\begin{cases}10 \text{ for } k\leq 941,\\ 11 \text{ for } k>941\end{cases}$	9	11

We get $\mathcal{B}_r\subseteq W_1$. For $s\in W'_1$, we infer from (7.1) that $\nu(s)=\nu_{\rm o}(s)\leq$

$G(k,s,\delta) := \min(f_0(k,s,\delta), G_1, G_2)$ where

$$(G_1,G_2) = \begin{cases} (f_1(k,s,3,2,\delta), \max_{p'\in\mathcal{P}} f_2(k,s,3,p',2,\delta)) & \text{for (ii)}, 8\nmid d,\\ (f_1(k,s,5,1,\delta), \max_{p'\in\mathcal{P}} f_2(k,s,5,p',1,\delta)) & \text{for (iii)}, 8\nmid d,\\ (f_1(k,s,3,1,3), \max_{p'\in\mathcal{P}} f_2(k,s,3,p',2,3)) & \text{for (ii)}, 8\mid d,\\ (f_1(k,s,5,1,3), \max_{p'\in\mathcal{P}} f_2(k,s,5,p',2,3)) & \text{for (iii)}, 8\mid d, \end{cases}$$

and when (iv) holds, $G_1 = G_2 = \max_{p'\in\mathcal{P}} f_1(k,s,p',1,\delta)$ if $2\,\|\,d$ or $4\,\|\,d$, $G_1 = G_2 = \max_{p'\in\mathcal{P}} f_2(k,s,7,p',1,3)$ if $8\mid d$. Hence

$$\xi_r \le g' + \sum_{s\in W_1'} (G(k,s,\delta)-1) =: \widetilde{\xi}_r.$$

Now we check that (7.4) holds, contradicting (6.1). Thus $p'\mid d$ for each prime $p'\in\mathcal{P}$.

Let r and g_1 be given by the following table:

Cases	(ii), (iii), $2\,\|\,d$	(ii), (iii), $4\,\|\,d$	(ii), $8\mid d$	(iv), $2\,\|\,d$	(iv), $8\mid d$
(r,g_1)	(12, 8)	(12, 4)	(15, 16)	(13, 4)	(17, 4)

Suppose that one of the above cases holds. Then $\mathcal{B}_r \subseteq \{s\in\mathcal{S}(r) : s\equiv 1 \pmod{2^\delta}, \left(\frac{s}{p'}\right) = 1,\ p'\in\mathcal{P}\cup\mathcal{P}_0\} = \{1\}\cup W''$ with $|W''| = g_1 - 1$ and $s \ge 2000/2^{3-\delta}$ for $s\in W''$. Thus $\xi_r \le \nu(1) + g_1 - 1$. From (7.1), we get $\nu(1) \le G(k)$ where $G(k) = f_1(k,1,3,2,\delta)$ if (ii) holds; $G(k) = f_1(k,1,5,2,\delta)$ if (iii) holds with $8\nmid d$; $G(k) = f_0(k,1,1)$ if (iv) holds with $2\,\|\,d$; $G(k) = f_1(k,1,7,2,3)$ if (iv) holds with $8\mid d$. Therefore $\xi_r \le G(k) + g_1 - 1 =: \widetilde{\xi}_r$ and we compute that (7.4) holds. This contradicts (6.1). Thus either (A): (iv) holds with $4\,\|\,d$, or (B): (iii) holds with $8\mid d$. Assume that $p'\nmid d$ with $p'\in\mathcal{P}_1$ where $\mathcal{P}_1 = \{23,29,31,37\}, \{11,13,17,19\}$ when (A), (B) holds, respectively. In the remaining part of this paragraph, by "respectively" we mean "when (A), (B) holds, respectively". We take $r = 18, 11$, respectively. Then $\mathcal{B}_r \subseteq \{s\in\mathcal{S}(r) : s\equiv 1 \pmod{2^\delta}, \left(\frac{s}{p'}\right) = 1, p'\in\mathcal{P}\cup\mathcal{P}_0\} \subseteq \{1,1705\}\cup W''$ with $|W''| = g_1$ and $s\ge 2000/2^{3-\delta}$ for $s\in W''$ where $g_1 = 3, 14$, respectively. Hence $\xi_r \le \nu(1)+\nu(1705)+g_1 \le G(k)+2+g_1 =: \widetilde{\xi}_r$, where $\nu(1) \le G(k) = \max_{p'\in\mathcal{P}_1} f_1(k,1,p',1,2), \max_{p'\in\mathcal{P}_1} f_2(k,1,5,p',1,3)$, respectively, by (7.1). We check that (7.4) holds, contradicting (6.1). Thus $p'\mid d$ with $p'\le 37$ if (A) holds and $p'\mid d$ with $p'\le 19$, $p'\ne 5$ if (B) holds. Now we take $r = 22, 16$, respectively, to get $\mathcal{B}_r \subseteq \{1\}\cup W''$ with $|W''| = g_2$ and $s\ge 2000/2^{3-\delta}$ for $s\in W''$ where $g_2 = 0, 3$, respectively. From (7.1), we get $\nu(1)\le G(k)$ with $G(k) = f_0(k,1,2), f_1(k,1,5,2,3)$, respectively. Hence $\xi_r \le G(k)+g_2 =: \widetilde{\xi}_r$ and we compute that (7.4) holds. This contradicts (6.1).

Thus it remains to consider case (iv) with $8\,|\,d$ and $7\,|\,d$. Then

$$a_i \equiv 1 \pmod 8 \quad \text{and} \quad \left(\frac{a_i}{p}\right) = 1 \quad \text{for } p = 3,5,7 \tag{7.5}$$

whenever $a_i \in R$. Let $k < 263$. By taking $r = 12$, we find that $\mathcal{B}_r \subseteq \big\{s \in \mathcal{S}(r) : s \equiv 1 \pmod 8, \big(\frac{s}{p_j}\big) = 1,\ 2 \le j \le 4\big\} = \{1, 6409, 9361, 12121, 214489, 268801, 4756609, 59994649\}$. Then by Lemma 7.3, $\nu(1) \le (k-1)/2$ since $k \nmid d$ by our assumption. Further, $\nu(6409)+\nu(268801)+\nu(4756609)+\nu(59994649) \le \lceil k/13\cdot 29\rceil \le 1$, $\nu(9361)+\nu(214489) \le \lceil k/11\cdot 37\rceil \le 1$ and $\nu(12121) \le 1$. Therefore $\xi_r \le (k-1)/2 + 3 =: \widetilde{\xi}_r$. We check that (7.4) holds contradicting (6.1). Thus $k \ge 263$. By (7.5), we see that a_i is not a prime ≤ 89. Hence for $a_i \in R$ with $P(a_i) \le 89$, we have $\omega(a_i) \ge 2$. Further, by (7.5), $a_i = p'q'$ with $11 \le p' \le 37$ and $41 \le q' \le 89$ is not possible. For integers P_1, P_2 with $P_1 < P_2$, let

$$\mathcal{I}(P_1,P_2) = \{i : p'q' \,|\, a_i,\ P_1 \le p' < q' \le P_2\}.$$

Then $|\mathcal{I}(P_1,P_2)| \le \sum_{P_1 \le p' < q' \le P_2} \lceil k/p'q' \rceil$. Suppose that $p_j \nmid d$ for some prime $j \in \{5,6\}$. Then $\nu(1) \le G_0(k) := \max_{j=5,6} f_1(k,1,p_j,2,3)$ by (7.1). We take $r = 23$. For $P_0 \in \{11,13\}$, let $A(P_0) = \{a_i : a_i = P_0 p'$ with $P_0 < p' \le 37$ or $a_i = P_0 p' q'$ with $P_0 < p' \le 37,\ 41 \le q' \le 83\}$. Then from (7.5), we get $A(11) \subseteq \{6721, 8569, 25201\}$ and $A(13) \subseteq \{17329, 17641, 27001\}$. Therefore we deduce from

$$\begin{aligned} I_r \subseteq\ & \{i : a_i = 1\} \cup \mathcal{I}(17,37) \cup \mathcal{I}(41,83) \\ & \cup \{i : a_i \in A(11) \cup A(13)\} \cup \{i : 11\cdot 13 p' \,|\, a_i, 17 \le p' \le 37\} \end{aligned}$$

that

$$\xi_r \le G_0(k) + \sum_{17 \le p' < q' \le 37} \left\lceil \frac{k}{p'q'} \right\rceil + \left\lceil \frac{k}{41\cdot 43} \right\rceil + 54 + 3 + 3 + 6 =: \widetilde{\xi}_r,$$

since $p'q' > k$ for $41 \le p' < q' \le 83$ except when $p' = 41$, $q' = 43$. Now we compute that (7.4) holds, contradicting (6.1). Thus $p_j \,|\, d$ for $j \le 6$. Assume that $p_j \nmid d$ for some j with $7 \le j \le 9$. Then $\nu(1) \le G_1(k) := \max_{7 \le j \le 9} f_1(k,1,p_j,1,3)$ by (7.1). We take $r = 24$. Then $I_r \subseteq \{i : a_i = 1\} \cup \mathcal{I}(17,37) \cup \mathcal{I}(41,89)$. It follows that $\xi_r \le G_1(k) + \sum_{17 \le p' < q' \le 37} \lceil k/p'q' \rceil + \lceil k/41\cdot 43\rceil + 65 =: \widetilde{\xi}_r$ and we check that (7.4) holds. This contradicts (6.1). Thus $p_j \,|\, d$ for $j \le 9$. Suppose that $p_j \nmid d$ for some j with $10 \le j \le 14$. Then $\nu(1) \le G_2(k) := \max_{10 \le j \le 14} f_1(k,1,p_j,1,3)$ by (7.1). We take $r = 21$. Then $\mathcal{B}_r \subseteq \big\{s \in \mathcal{S}(r) : s \equiv 1 \pmod 8$ and $\big(\frac{s}{p_i}\big) = 1,\ i \le 9\big\} = \{1, 241754041\}$, giving $\xi_r \le G_2(k) + 1 =: \widetilde{\xi}_r$. Now we check that (7.4) holds, contradicting (6.1). Hence $p_j \,|\, d$ for $j \le 14$. Suppose that $p_j \nmid d$ for some j with $15 \le j \le 22$. Then $\nu(1) \le G_3(k) := \max_{15 \le j \le 22} f_1(k,1,p_j,1,3)$ by (7.1). We take $r = 26$.

Then $\mathcal{B}_r \subseteq \{1\}$ as above, giving $\xi_r \le G_2(k) =: \widetilde{\xi}_r$. We compute that (7.4) holds, contradicting (6.1). Thus $p_j \,|\, d$ for $j \le 22$. Finally, we take $r = 32$. Then $\mathcal{B}_r \subseteq \{1\}$ as above, giving $\xi_r \le \nu(1) \le \frac{(k-1)}{2} =: \widetilde{\xi}_r$ by Lemma 7.3. We check that (7.4) holds. This contradicts (6.1). ∎

LEMMA 7.6. *We have*

(7.6) $$k - |R| \ge g \quad \textit{for } k \ge k_0(g),$$

where g and $k_0(g)$ are given by

(i)

g	9	14	17	29	33	61	65	129	256	2^s with $s \ge 9$, $s \in \mathbb{Z}$
$k_0(g)$	101	299	308	489	556	996	1057	2100	4252	$s2^{s+1}$

(ii) d *even*:

g	18	29	33	61	64	128	256	512	1024
$k_0(g)$	101	223	232	409	430	900	1895	4010	8500

(iii) $4 \,\|\, d$:

g	26	32	33	61	64	128	256	512	1024
$k_0(g)$	101	126	129	286	303	640	1345	2860	6100

(iv) $8 \,|\, d$:

g	33	61	64	128	256	512	1024
$k_0(g)$	101	209	220	466	990	2110	4480

(v) $3 \,|\, d$:

g	26	32	33	64	125	128	256	512
$k_0(g)$	101	126	129	351	720	735	1550	3300

(vi) $p \,|\, d$ *with* $p \in \{5, 7\}$:

g	33	64	128	256
$k_0(g)$	240	460	930	1940

Further, we have $k_0(128) = 1200$ *if* $p \,|\, d$ *with* $p \le 19$ *and* $k_0(256) = 2870$ *if* $p \,|\, d$ *with* $p \le 47$.

(vii) *Further,* $k_0(256) = 1115$ *if* $pq \,|\, d$ *with* $p \in \{5, 7, 11\}$; $k_0(256) = 1040$ *if* $2p \,|\, d$ *with* $p \in \{3, 5\}$; $k_0(512) = 1400$ *if* $105 \,|\, d$; $k_0(512) = 1440$ *if* $30 \,|\, d$; *and* $k_0(512) = 1480$ *if* $8p \,|\, d$ *with* $p \in \{3, 5\}$.

Proof. (i) Let g be given as in (i). Assume that $k \ge k_0(g)$ and $k - |R| < g$. We shall arrive at a contradiction.

Let $g \ne 9$. From (5.1), we have $\prod_{a_i \in R} a_i \ge (1.6)^{|R|}(|R|)!$ whenever $|R| \ge 286$. We observe that (5.3) and (5.4) hold with $i_0 = 0$, $h_0 = 286$, $z_1 = 1.6$,

$g_1 = g-1$, $\mathfrak{m} = \min(89, \sqrt{k_0(g)})$, $\ell = 0$, $\mathfrak{n}_0 = 1$, $\mathfrak{n}_1 = 1$ and $\mathfrak{n}_2 = 2^{1/6}$ for $k \ge g_1 + 286$ and thus for $k \ge k_0(g)$.

Let $g = 2^s$ with $s \ge 9$. Then $g_1/k \le 2^s/s2^{s+1} \le 1/18$ and from (5.4) we get

$$2^s - 1 > \frac{c_1 k - c_2 \log k - c_3}{\log c_4 k} = \frac{c_1 k - c_3 + c_2 \log c_4}{\log c_4 k} - c_2 \tag{7.7}$$

where

$$c_1 = \log\left(\frac{1.6}{2.71851}\prod_{p\le\mathfrak{m}} p^{\frac{2}{p^2-1}}\right) + \log\left(1-\frac{1}{18}\right), \qquad c_2 = 1.5\pi(\mathfrak{m}) - 1,$$

$$c_3 = \log\left(2^{1/6}\prod_{p\le\mathfrak{m}} p^{0.5+\frac{2}{p^2-1}}\right) - \frac{1}{2}\log\left(1-\frac{1}{18}\right), \quad c_4 = \frac{1.6}{e}.$$

Here we check that $c_1 k - c_2 \log k - c_3 > 0$ at $k = 9\cdot 2^{10}$ and hence (7.7) is valid. Further, we observe that the right hand side of (7.7) is an increasing function of k. Putting $k = k_0(g) = s2^{s+1}$, we deduce from (7.7) that

$$2^s\left\{\frac{2c_1 - \frac{c_3 - c_2\log c_4}{s2^s}}{\log 2 + \frac{\log(2c_4 s)}{s}} - \frac{c_2-1}{2^s} - 1\right\} < 0.$$

The expression inside the braces is an increasing function of s and it is positive at $s = 9$. Hence (7.7) does not hold for all $k \ge k_0(g)$. Therefore $k - |R| \ge g = 2^s$ whenever $s \ge 9$ and $k \ge s2^{s+1}$.

Let $g \in \{14, 17, 29, 33, 61, 65, 129, 256\}$ and $k_1(g) = 299, 316, 500, 569, 1014, 1076, 2126, 4295$ according as $g = 14, 17, 29, 33, 61, 65, 129, 256$. We see that the right hand side of (5.4) is an increasing function of k and we check that it exceeds g_1 at $k = k_1(g)$. Therefore (5.4) is not possible for $k \ge k_1(g)$. Thus $g \ne 14$ and $k < k_1(g)$. For every k with $k_0(g) \le k < k_1(g)$, we compute the right hand side of (5.3) and we find it greater than g_1. This is not possible.

Thus we may assume that $g = 9$ and $k < 299$. By taking $r = 4$ for $101 \le k \le 181$ and $r = 5$ for $181 < k < 299$ in (6.3) and (6.5), we get $k - |R| \ge k - F'(k,r) - 2^r \ge 9$ for $k \ge 101$ except when $103 \le k \le 120$, $k \ne 106$ where $k - |R| \ge k - F(k,r) - 2^r \ge k - F'(k,r) - 2^r = 8$. Let $103 \le k \le 120$, $k \ne 106$. We may assume that $k - |R| = 8$ and hence $F(k,r) = F'(k,r)$. Thus for each prime $11 \le p \le k$, there are exactly σ_p many i's for which $p \mid a_i$ and, for any i, $pq \nmid a_i$ whenever $11 \le q \le k$, $q \ne p$. Now we get a contradiction by considering the i's for which a_i's are divisible by primes $17, 101; 103, 17; 13, 103;$ $53, 13;$ $107, 53;$ $11, 109;$ $37, 11;$ $19, 113;$ $23, 19;$ $29, 23;$ $13, 29;$ $59, 13;$ $17, 59$ when $k = 103, 104, 105, 107, 108, 111, 112, 115, 116, 117, 118, 119, 120$, respectively; $107, 53, 13, 103, 17$ when $k = 109$; $109, 107, 53$ when $k = 110$; $37, 11, 109, 107$ when $k = 113$; and $113, 37, 11$ when $k = 114$. For instance, let $k = 113$. Then $37 \mid a_i$ for $i \in \{0, 37, 74, 111\}$ or $i \in \{1, 38, 75, 112\}$. We consider the first case; the other case follows similarly. Then $11\,|\,a_i$ for $i \in \{2+11j : 0 \le j \le 10\}$ and $109\,|\,a_i$ for $i \in \{1, 110\}$. Now $\sigma_{107} = 2$ implies that $107\,|\,a_i a_{i+107}$ for $i \in \{j : 0 \le j \le 5\}$, a contradiction. The other cases are excluded similarly.

(ii) Let d be even and g be given as in (ii). Assume that $k \ge k_0(g)$ and $k - |R| < g$. From (5.2), we have $\prod_{a_i \in R} a_i \ge (2.4)^{|R|}(|R|)!$ whenever $|R| \ge 200$. By taking $i_0 = 0$, $h_0 = 200$, $\mathfrak{m} = \sqrt{k_0(g)}$, $z_1 = 2.4$, $\ell = 1$, $\mathfrak{n}_0 = 2^{1/3}$, $\mathfrak{n}_1 = 2^{1/6}$ and $\mathfrak{n}_2 = 1$, we observe that (5.3) and (5.4) are valid for $k \ge g - 1 + 200$. Let $g \in \{33, 61, 64, 128, 256, 512, 1024\}$. Thus (5.3) and (5.4) are valid for $k \ge k_0(g)$. Let $k_1(g) = 232, 414, 435, 904, 1907, 4024, 8521$ according as $g = 33, 61, 64, 128, 256, 512, 1024$. We see that (5.4) is not possible for $k \ge k_1(g)$. Therefore $g \ne 33$ and $k < k_1(g)$. For every k with $k_0(g) \le k < k_1(g)$, we check that (5.3) is contradicted. Therefore $g \in \{18, 29\}$ and we may assume that $k < 232$. We take $r = 5$ for $101 \le k < 200$ and $r = 6$ for $200 \le k < 232$. From (6.10) and (6.6), we get $k - |R| \ge k - F'(k, r) - 2^{r-1}$. We compute that $k - F'(k, r) - 2^{r-1} \ge 18, 29$ for $k \ge 101, 217$, respectively. Hence (ii) follows.

(iii), (iv) Let g be given as in (iii), (iv). Suppose that $k \ge k_0(g)$ and $k - |R| < g$. We have $\prod_{a_i \in R} a_i \ge (2^\delta)^{|R|-1}(|R| - 1)!$ since $a_i \equiv n \pmod{2^\delta}$. We take $z_1 = 4$ if $4\,\|\,d$ and $z_1 = 8$ if $8\,|\,d$. We observe that (5.3) and (5.4) are valid for $k \ge k_0(g)$ with $i_0 = 1$, $h_0 = 1$, $\mathfrak{m} = \sqrt{k_0(g)}$, $z_1 = 2$, $\ell = 1$, $\mathfrak{n}_0 = 2^{1/3}$, $\mathfrak{n}_1 = 2^{1/6}$ and $\mathfrak{n}_2 = 1$.

Let $4\,\|\,d$ and $g \in \{61, 64, 128, 256, 512, 1024\}$. Let $k_1(g) = 288, 306, 640, 1350, 2870, 6100$ according as $g = 61, 64, 128, 256, 512, 1024$. We see that (5.4) is not possible for $k \ge k_1(g)$. Therefore $g \ne 128, 1024$ and $k < k_1(g)$. For every k with $k_0(g) \le k < k_1(g)$, we check that (5.3) is contradicted.

Let $8\,|\,d$ and $g \in \{61, 64, 128, 256, 512, 1024\}$. Let $k_1(g) = 210, 221, 468, 994, 2111, 4485$ according as $g = 61, 64, 128, 256, 512, 1024$. We see that (5.4) is not possible for $k \ge k_1(g)$. Therefore $k < k_1(g)$. For every k with $k_0(g) \le k < k_1(g)$, we check that (5.3) is contradicted.

Thus we may assume that $g \in \{26, 32, 33\}$, $k < 286$ if $4\,\|\,d$ and $g = 33$, $k < 209$ if $8\,|\,d$. By taking $r = 6$ for $101 \le k < 286$, we deduce from (6.10) and (6.6) that $k - |R| \ge k - F'(k, r) - 2^{r-\delta} \ge g$ for $k \ge k_0(g)$. Hence the assertions (iii) and (iv) follow.

(v) Let $3\,|\,d$. Suppose that $k \ge k_0(g)$ and $k - |R| < g$. We have $\prod_{a_i \in R} a_i \ge 3^{|R|-1}(|R| - 1)!$ since $a_i \equiv n \pmod 3$. We observe that (5.3) and (5.4) are valid with $i_0 = 1$, $h_0 = 1$, $\mathfrak{m} = \sqrt{k_0(g)}$, $z_1 = 3$, $\ell = 1$, $\mathfrak{n}_0 = 3^{1/4}$, $\mathfrak{n}_1 = 3^{1/4}$ and $\mathfrak{n}_2 = 2^{1/6}$. Let $g \in \{64, 125, 128, 256, 512\}$, and $k_1(g) = 354, 720, 737, 1556, 3300$ according as $g = 64, 125, 128, 256, 512$. We see that (5.4) is not possible for $k \ge k_1(g)$. Therefore $g \ne 125, 512$ and $k < k_1(g)$. For every k with $k_0(g) \le k < k_1(g)$, we check that (5.3) is contradicted.

Thus it remains to consider $g\in\{26,32,33\}$ and $k<351$. We take $r=6$ for $101\le k<351$. We see from (6.10) and (6.13) with $p=3$ that $k-|R|\ge k-F'(k,r)-2^{r-2}\ge g$ for $k\ge k_0(g)$.

(vi) Suppose $g\in\{33,64,128,256\}$, $k\ge k_0(g)$ and $k-|R|<g$. By (ii) and (v), we may assume that $2\nmid d$ and $3\nmid d$. We observe that

$$\prod_{a_i\in R}a_i\ge\left(\frac{2p}{p-1}\right)^{|R|-(p-1)/2}\left(|R|-\frac{p-1}{2}\right)!$$

since the number of quadratic residues or quadratic non-residues mod p is $(p-1)/2$. Let $p\,|\,d$ with $p\le p'$. Then

$$\left(\frac{2p}{p-1}\right)^{|R|-(p-1)/2}\left(|R|-\frac{p-1}{2}\right)!\ge\left(\frac{2p'}{p'-1}\right)^{|R|-(p'-1)/2}\left(|R|-\frac{p'-1}{2}\right).$$

We take $p'=7,\ 19$ and 47 in the first, second and third case, respectively. Then (5.3) and (5.4) are valid with $z_1=2p'/(p'-1)$, $i_0=h_0=(p'-1)/2$, $\mathfrak{m}=\sqrt{k_0(g)}$, $\ell=1$, $\mathfrak{n}_0=(p')^{1/(p'+1)}$, $\mathfrak{n}_1=5^{1/3}$ and $\mathfrak{n}_2=2^{1/6}$. We find that (5.4) is not possible for $k\ge k_0(g)+24$ and (5.3) is not possible for each k with $k_0(g)\le k<k_0(g)+24$. This is a contradiction.

(vii) Let $(z_1,i_0,\ell',\mathfrak{n}'_0,\mathfrak{n}'_1,\mathfrak{n}'_2)$ be given by

	$pq\,\|\,d$	$2^\delta p\,\|\,d$	$105\,\|\,d$	$30\,\|\,d$
	$p,q\in\{5,7,11\}$	$p\in\{3,5\},\ \delta\in\{1,3\}$		
(z_1,i_0)	$(77/15,15)$	$(2^{\delta-1}5,2)$	$(35/2,6)$	$(15,2)$
ℓ'	2	2	3	3
$\mathfrak{n}'_0$	$z_2(7)z_2(11)$	$z_2(2)z_2(5)$	$z_2(3)z_2(5)z_2(7)$	$z_2(2)z_2(3)z_2(5)$
$\mathfrak{n}'_1$	$z_3(5)z_3(7)$	$z_3(2)z_3(3)$	$z_3(3)z_3(5)z_3(7)$	$z_3(2)z_3(3)z_3(5)$
$\mathfrak{n}'_2$	$2^{1/6}$	1	$2^{1/6}$	1

where $z_2(p)=p^{1/(p+1)}$, $z_3(p)=p^{(p-1)/2(p+1)}$. We observe that $\prod_{a_i\in R}a_i\ge z_1^{|R|-i_0}(|R|-i_0)!$ with (z_1,i_0) given above. Suppose $g\in\{256,512\}$, $k\ge k_0(g)$ and $k-|R|<g$. We see that (5.3) and (5.4) are valid for $k\ge k_0(g)$ with $h_0=i_0$, $\mathfrak{m}=\sqrt{k_0(g)}$, $\ell=\ell'$, $\mathfrak{n}_0=\mathfrak{n}'_0$, $\mathfrak{n}_1=\mathfrak{n}'_1$ and $\mathfrak{n}_2=\mathfrak{n}'_2$. We find that (5.4) is not possible for $k\ge k_0(g)+2$ and (5.3) is not possible for each k with $k_0(g)\le k<k_0(g)+2$. This is a contradiction. ∎

8. Further lemmas. We observe that (3.24) is satisfied when $k\ge 11$ by Lemma 4.2. We shall use it without reference in this section.

LEMMA 8.1. *Let d be odd and p,q be primes dividing d. Let $\omega(d)\le 4$ and $k\le 821$. Assume that $g_{p,q}(r)\le 2^{r-\omega(d)}$ for $r=5,6$. Then* (1.1) *with $k\ge 101$ has no solution.*

Proof. Suppose equation (1.1) has a solution. Let $r=5$ if $101\le k<257$ and $r=6$ if $257\le k\le 821$. From (6.9), $\nu(a_i)\le 2^{\omega(d)}$ and (6.1), we get

$k-F'(k,r) \le \xi_r \le 2^{\omega(d)} g_{p,q} \le 2^r$. We find $k-F'(k,r) > 2^r$ by computation. This is a contradiction. ∎

LEMMA 8.2. *Equation* (1.1) *with* $k \ge 101$ *and* $\omega(d) \le 4$ *is not possible.*

Proof. We may assume that k is prime by Lemma 7.4. Let d be even. For $k-|R| \ge \mathfrak{h}(5) = 4(2^{\omega(d)-\theta}-1)+1$, we see from Corollary 3.10 with $z_0 = 5$ that $n+(k-1)d < (3/Q)k^3$ with $Q = 32$ if $2 \parallel d$ and 16 if $4 \mid d$. Let $\omega(d) \le 3$. Since $k - |R| \ge \mathfrak{h}(5)$ by Lemma 7.6(ii)–(iv) and $|S_1| \ge |T_1|/2^{\omega(d)-\theta} \ge 0.3k/2^{3-\theta}$ by Lemma 4.3, we get $(3/Q)k^3 > n + (k-1)d > 2^{\delta}(0.3k/2^{3-\theta} - 1)k^2$, a contradiction. Thus $\omega(d) = 4$. Let $k \ge 710$. Then $k - |R| \ge \mathfrak{h}(5)$ by Lemma 7.6 and $|S_1| \ge |T_1|/2^{\omega(d)-\theta} \ge 0.4k/2^{4-\theta}$ by Lemma 4.3. Hence we get $3/Q > n + (k-1)d > 2^{\delta}(0.4k/2^{4-\theta} - 1)k^2$, a contradiction again. Therefore $k < 710$. By Lemma 7.6, we get $k - |R| \ge \mathfrak{h}(3)$, implying $d < \frac{3}{16}k^2$ if $2 \parallel d$ and $d < \frac{3}{4}k^2$ if $4 \mid d$ by Corollary 3.10 with $z_0 = 3$. However, $d \ge 2^{\delta} \cdot 53 \cdot 59 \cdot 61$ by Lemma 7.5(c). This is a contradiction.

Thus d is odd. Suppose $|S_1| \le |T_1| - \mathfrak{h}(3)$. By Lemma 3.12, we have

$$d < \frac{\varrho}{48}\, k^2, \quad n + (k-1)d < \frac{\varrho}{48}\, k^3. \tag{8.1}$$

Let $k \ge 710$. Since $\nu(a_i) \le 2^{\omega(d)}$, we derive from Lemma 4.3 that $|S_1| \ge |T_1|/2^{\omega(d)} > 0.4k/16 = 0.025k$. Therefore $\max_{A_i \in S_1} A_i > \varrho(0.025k - 1)$, giving $n + (k-1)d > \varrho(0.025k - 1)k^2$, which contradicts (8.1). Thus we have $k < 710$. We see from Lemma 4.3 that $|T_1| > 0.3k$. For $\omega(d) \le 3$, we have $\max_{A_i \in S_1} A_i > \varrho(0.3k/8-1)$, giving $n + (k-1)d > \varrho(0.3k/8 - 1)k^2$, which contradicts (8.1). Let $\omega(d) = 4$. By Lemma 7.5(a), we see that $d \ge \min(3 \cdot 53 \cdot 59 \cdot 61, 23 \cdot 29 \cdot 31 \cdot 37) > \frac{3}{48}k^2$, contradicting (8.1).

Hence $|S_1| \ge |T_1| - \mathfrak{h}(3) + 1$. Therefore

$$n + (k-1)d \ge \varrho(|T_1| - \mathfrak{h}(3))k^2. \tag{8.2}$$

Let $k-|R| \ge \mathfrak{h}(5)$. By Corollary 3.10 with $z_0 = 5$, we get $n+(k-1)d < \frac{3}{16}k^3$, which, together with $|T_1| \ge 0.3k$, by Lemma 4.3, contradicts (8.2) when $\omega(d) \le 2$. Further, $k \le 133, 275$ when $\omega(d) = 3, 4$, respectively. Thus either

$$k - |R| < \mathfrak{h}(5) \tag{8.3}$$

or

$$\omega(d) > 2; \quad k \le 131 \quad \text{if } \omega(d) = 3; \quad k \le 271 \quad \text{if } \omega(d) = 4. \tag{8.4}$$

We now apply Lemma 7.6(i) to get $\omega(d) \ge 2$ and $k \le 293, 487, 991$ for $\omega(d) = 2, 3, 4$, respectively.

Let $3 \mid d$. Then we find from Lemma 7.6(v) that $\omega(d) > 2$ and $k \le 131, 350$ when $\omega(d) = 3, 4$, respectively. By Lemma 7.5, we get $\mathfrak{p}_2 \ge 53$ and hence $53 \le \mathfrak{p}_2 \le (d/3)^{1/(\omega(d)-1)}$. By Corollary 3.10 with $z_0 = 3$ if $\omega(d) = 3$, $z_0 = 2$ if $\omega(d) = 4$ and Lemma 7.6(v), we get $d < \frac{3}{4}k^2$ if $\omega(d) = 3$ and $< 3k^2$ if $\omega(d) = 4$. Therefore $53 \le \mathfrak{p}_2 < k/2 < 67$ if $\omega(d) = 3$ and $53 \le \mathfrak{p}_2 < k^{2/3} \le$

$350^{2/3} < 53$ if $\omega(d)=4$. Therefore $\omega(d)=3$ and $53 \le \mathfrak{p}_2 \le 61$. Now we get a contradiction from Lemma 8.1 with $(p,q)=(3,\mathfrak{p}_2)$ and (6.14).

Thus we may assume that $3 \nmid d$. Therefore $k \le 293, 487, 991$ for $\omega(d) = 2,3,4$, respectively, as stated above. Let $\omega(d)=4$ and $k<308$. From $k-|R| \ge 9$ by Lemma 7.6(i) and by Corollary 3.11, there exists a partition (d_1,d_2) of d such that $\max(d_1,d_2) < (k-1)^2$. Thus $\mathfrak{p}_1\mathfrak{p}_2 \le \max(d_1,d_2) < (k-1)^2$, giving $\mathfrak{p}_1 < k-1$. By taking $r=5$ for $101 \le k < 251$, $r=6$ for $251 \le k < 308$, we see from (6.10) and $g_{\mathfrak{p}_1} \le 2^{r-1}$ by (6.13) with $p=\mathfrak{p}_1$ that $k-|R| \ge k-F'(k,r)-2^{r-1} \ge 16$. Now we return to $\omega(d)=2,3,4$. By Lemma 7.6(i), we get $k-|R| \ge 2^{\omega(d)}$. Then we see from Corollary 3.10 with $z_0=2$ that there is a partition (d_1,d_2) of d with $d_1<k-1$, $d_2<4(k-1)$. Thus $\mathfrak{p}_1<k$. We take $r=5$ for $101 \le k < 211$ and $r=6$ for $211 \le k < 556$ for the next computation and we use Lemma 7.6(i) for $k \ge 556$. From (6.10) with $p=q=\mathfrak{p}_1$ and (6.13) with $p=\mathfrak{p}_1$, and since $\sum_{p|d,\,p>p_r}\sigma_p - g_{\mathfrak{p}_1} \ge 2-2^{r-1}$ if $\mathfrak{p}_1>p_r$ and $\ge -2^{r-2}$ if $\mathfrak{p}_1 \le p_r$, we get

$$(8.5) \qquad k-|R| \ge k-F'(k,r)+2-2^{r-1} \ge \begin{cases} 20 & \text{for } k \ge 101, \\ 29 & \text{for } k \ge 211, \\ 33 & \text{for } k \ge 251. \end{cases}$$

Therefore we find from (8.3) and (8.4) that $\omega(d)>2$ and $k \le 199, 991$ when $\omega(d)=3,4$, respectively.

Let $\omega(d)=3$. By Corollary 3.10 with $z_0=3$, there is a partition (d_1,d_2) with $d_1<(k-1)/2$ and $d_2<2(k-1)$. Thus $\mathfrak{p}_1\mathfrak{p}_2 \le \max(d_1,d_2) < 2(k-1)$, giving $\mathfrak{p}_1 < \sqrt{2(k-1)} \le \sqrt{2\cdot 198}$ and hence $p_1 \le 19$. Further, the possibility $p_1=19$ is excluded since $19\cdot 23 > 2(k-1)$. Also, $\mathfrak{p}_2 \le 79, 53, 31, 29, 23$ for $\mathfrak{p}_1 = 5,7,11,13,17$, respectively. Now we apply Lemma 7.5(a) to derive that either $\mathfrak{p}_1=5$, $53 \le \mathfrak{p}_2 \le 79$ or $\mathfrak{p}_1=7$, $\mathfrak{p}_2=53$. Further, from $5\cdot 53 < 2(k-1)$, we get $k \ge 134$. Thus $k-|R| \le 28$ by (8.3) and (8.4). Now we take $r=6$ for $134 \le k \le 199$ in the next computation. We see from (6.10) and (6.14) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $k-|R| \ge k-F'(k,r)-2^{r-2} \ge 29$. This is a contradiction.

Let $\omega(d)=4$. By Lemma 7.5(a), (b), we get $d \ge \min(5\cdot 53\cdot 59\cdot 61, 23\cdot 47\cdot 53\cdot 59, 31\cdot 41\cdot 47\cdot 53) = 953735$. Further, by Corollary 3.10 with $z_0=2$ if $k<251$, $z_0=3$ if $k \ge 251$ and by (8.5), we obtain $d<3k^2$ if $k<251$ and $d<\frac{3}{4}k^2$ for $k \ge 251$. This is a contradiction since $k \le 991$. ∎

LEMMA 8.3. *Assume* (1.1) *with* $\omega(d) \ge 12$. *Suppose that*

$$(8.6) \qquad d < \frac{3}{16}k^2, \qquad n+(k-1)d < \frac{3}{16}k^3.$$

Then $k < \omega(d)4^{\omega(d)}$.

Proof. Assume that $k \geq \omega(d)4^{\omega(d)}$. Then from $40\cdot\left(\frac{3}{16}\right)^{2/11} < 12^{7/11}2^{36/11}$ and $\omega(d) \geq 12$, we get $(3k^2/16)^{2/11} \leq k/(40\cdot 2^{\omega(d)})$. This together with $\mathfrak{q}_1\mathfrak{q}_2 \leq (d/2^{\delta\theta})^{2/(\omega(d)-\theta)} < (3k^2/16)^{2/11}$ by (2.9) and (8.6) gives $\mathfrak{q}_1\mathfrak{q}_2 < k/(40\cdot 2^{\omega(d)})$. Hence we derive from Corollary 3.7(ii) with $d' = \mathfrak{q}_1\mathfrak{q}_2$ that

$$\nu(A_i) \leq 2^{\omega(d)-2-\theta} \quad \text{whenever} \quad A_i \geq \frac{k}{40\cdot 2^{\omega(d)}}. \tag{8.7}$$

Let

$$T^{(1)} = \left\{ i \in T_1 : A_i > \frac{2^\delta \varrho k}{6\cdot 2^{\omega(d)}} \right\}, \qquad T^{(2)} = T_1 \setminus T^{(1)} \tag{8.8}$$

and

$$S^{(1)} = \{A_i : i \in T^{(1)}\}, \qquad S^{(2)} = \{A_i : i \in T^{(2)}\}. \tag{8.9}$$

Then considering residue classes modulo $2^\delta\varrho$, we derive that

$$\frac{2^\delta \varrho k}{6\cdot 2^{\omega(d)}} \geq \max_{A_i\in S^{(2)}} A_i \geq 2^\delta\varrho(|S^{(2)}|-1)+1$$

so that $|S^{(2)}| \leq k/(6\cdot 2^{\omega(d)}) + 1 \leq k/(6\cdot 2^{\omega(d)}) + 1$. We deduce from (8.8), (8.9) and (8.7), together with $\nu(A_i) \leq 2^{\omega(d)}$ by Corollary 3.7(ii), that

$$\begin{aligned} |T^{(2)}| &\leq \frac{k}{40\cdot 2^{\omega(d)}}\, 2^{\omega(d)} + \left(\frac{k}{6\cdot 2^{\omega(d)}} - \frac{k}{40\cdot 2^{\omega(d)}} + 1\right)2^{\omega(d)-2} \\ &\leq \frac{k}{40} + \frac{1}{4}\left(\frac{k}{6} - \frac{k}{40}\right) + 2^{\omega(d)-2} \leq \frac{k}{24} + \frac{3k}{160} + \frac{k}{480} = \frac{k}{16} \end{aligned}$$

since $k \geq \omega(d)4^{\omega(d)}$ and $\omega(d) \geq 12$. By Lemma 4.3 and $k > 1639$, we have

$$|T^{(1)}| > |T_1| - |T^{(2)}| \geq 0.42k - \frac{k}{16} = 0.3575k.$$

Let $\mathfrak{C}$, $\mathfrak{C}_\mu$ be as in Lemma 5.5 with $c = 2$. Then

$$\begin{aligned} 0.3575k < |T^{(1)}| &= |S^{(1)}| + \sum_{\mu\geq 2}(\mu-1)|\mathfrak{C}_\mu| \leq |S^{(1)}| + \mathfrak{C} \\ &\leq |S^{(1)}| + \frac{3\log 2}{16}\,\omega(d)4^{\omega(d)} \end{aligned}$$

by Lemma 5.5. Now we use $(3\log 2)/16 < 1/7.6$ to get $0.3575k < |S^{(1)}| + k/7.6$, implying $|S^{(1)}| > 0.2259k$. Therefore $n+(k-1)d \geq (\max_{A_i\in S^{(1)}} A_i)k^2 \geq 0.2259k^3$, contradicting (8.6). ∎

LEMMA 8.4. *Assume* (1.1) *with* $\omega(d) \geq 5$. *Then there is no non-degenerate double pair.*

Proof. Assume (1.1) with $\omega(d) \geq 5$. Further, we suppose that there exists a non-degenerate double pair. Then we derive from Lemma 3.4 with $z_0 = 2$

that

$$d < \mathcal{X}_0 k^2, \qquad n+(k-1)d < \mathcal{X}_0 k^3, \tag{8.10}$$

where

$$\mathcal{X}_0 = 3, 3/2, 12, 6 \quad \text{if } 2\nmid d,\ 2\,\|\,d,\ 4\,\|\,d,\ 8\,|\,d, \text{ respectively.} \tag{8.11}$$

This with $d \geq 2^{\delta}\prod_{i=2}^{\omega(d)+1-\delta'} p_i$ implies $k^2 > \frac{1}{6}\prod_{i=1}^{\omega(d)} p_i$. Therefore we see from Lemma 5.1(ii), (iv) that

$$\log\left(\frac{k}{\omega(d)2^{\omega(d)}}\right) \geq \omega(d)\left\{\frac{\log\omega(d)+\log\log\omega(d)-1.076868}{2} - \log 2 - \frac{\log\omega(d)}{\omega(d)}\right\} - \frac{\log 6}{2}.$$

The right side of the above inequality is an increasing function of $\omega(d)$ and hence $k > 9\omega(d)2^{\omega(d)}$ for $\omega(d) \geq 12$. We deduce from $\mathcal{X}_0 k^2 > d \geq 2^{\delta}\prod_{i=2}^{\omega(d)+1-\delta'} p_i$ that $k > 3.2\omega(d)2^{\omega(d)}$ if $\omega(d) = 10, 11$. Further, $k > 2.97\omega(d)2^{\omega(d)}$ if $\omega(d) = 8, 9$ when d is odd. Also, $k > 2542, 12195$ when $\omega(d) = 8, 9$, respectively, if $2\,\|\,d$ or $8\,|\,d$ and $k > 1271, 6097$ when $\omega(d) = 8, 9$, respectively, if $4\,\|\,d$.

Suppose $k < 1733$. Then $\omega(d) \leq 8$ if $4\,\|\,d$ and $\omega(d) < 8$ otherwise. By Lemma 7.5(a), (c), we get $d \geq \min(3\cdot 53\cdot 59\cdot 61\cdot 67, 23\cdot 29\cdot 31\cdot 37\cdot 41)$ if d is odd and $d \geq 2^{\delta}\cdot 53\cdot 59\cdot 61\cdot 67$ if d is even. This is not possible since $d < \mathcal{X}_0 k^2$. Hence $k \geq 1733$.

Let d be even and $\omega(d) = 8, 9$. Since $k \geq 1733$, we get $k - |R| \geq \mathfrak{h}(3)$ by Lemma 7.6(ii)–(iv), implying $d < \frac{3}{16}k^2, \frac{3}{4}k^2$ if $2\,\|\,d$, $4\,|\,d$, respectively, by Corollary 3.10 with $z_0 = 3$. Therefore $k \geq 2.48\omega(d)2^{\omega(d)}$ if $4\,\|\,d$ and $k \geq 3.2\omega(d)2^{\omega(d)}$ otherwise.

Therefore for $\omega(d) \geq 8$, we have

$$k \geq \begin{cases} 2.48\omega(d)2^{\omega(d)} & \text{if } 4\,\|\,d, \\ 2.97\omega(d)2^{\omega(d)} & \text{if } d \text{ is odd, } \omega(d) = 8, 9, \\ 3.2\omega(d)2^{\omega(d)} & \text{otherwise.} \end{cases} \tag{8.12}$$

Suppose that $|S_1| \leq |T_1| - \mathfrak{h}(3)$ if d is odd and $|S_1| \leq |T_1| - \mathfrak{h}(5)$ if d is even. We put

$$\mathcal{X} := \begin{cases} \varrho/48 & \text{if } \mathrm{ord}_2(d) \leq 1, \\ 1/12 & \text{if } \mathrm{ord}_2(d) \geq 2,\ 3\nmid d, \\ 3/16 & \text{if } \mathrm{ord}_2(d) \geq 2,\ 3\,|\,d. \end{cases}$$

Then

$$d < \mathcal{X}k^2, \qquad n+(k-1)d < \mathcal{X}k^3 \tag{8.13}$$

by Lemma 3.12. Therefore $k < \omega(d)4^{\omega(d)}$ for $\omega(d) \geq 12$ by Lemma 8.3.

Let $\omega(d) \geq 19$. Then

$$\Big(2^{\delta}\prod_{i=2}^{9} p_i\Big)29^{\omega(d)-8-\delta'} \leq d < \mathcal{X}k^2$$
$$< W := \begin{cases} \frac{3}{48}\omega(d)^2 16^{\omega(d)} & \text{if } \mathrm{ord}_2(d) \leq 1, \\ \frac{3}{16}\omega(d)^2 16^{\omega(d)} & \text{if } \mathrm{ord}_2(d) \geq 2. \end{cases}$$

Therefore

$$\frac{29}{16} < \left(\left(64\prod_{i=3}^{9} p_i\right)^{-1} 29^9\omega(d)^2\right)^{1/\omega(d)}.$$

We see that the right hand side of the above inequality is a non-increasing function of $\omega(d)$ and the inequality does not hold at $\omega(d) = 26$. Thus $\omega(d) \leq 25$. Further, we get a contradiction from $2^{\delta}\prod_{i=2}^{\omega(d)+1-\delta'} p_i \leq d < W$ since $\omega(d) \geq 19$.

Thus $\omega(d) \leq 18$. We deduce from (2.9) and $d < \mathcal{X}k^2$ that

$$\mathfrak{q}_1 \cdots \mathfrak{q}_h < \mathcal{X}_1^h := \begin{cases} \left(\frac{\varrho}{48}\right)^{h/\omega(d)} k^{2h/\omega(d)} & \text{if } d \text{ is odd}, \\ \left(\frac{\varrho}{96}\right)^{h/(\omega(d)-1)} k^{2h/(\omega(d)-1)} & \text{if } 2 \,\|\, d, \\ \left(\frac{1}{12\cdot 4^{\theta}}\right)^{h/(\omega(d)-\theta)} k^{2h/(\omega(d)-\theta)} & \text{if } 4 \mid d,\ 3 \nmid d, \\ \left(\frac{3}{16\cdot 4^{\theta}}\right)^{h/(\omega(d)-\theta)} k^{2h/(\omega(d)-\theta)} & \text{if } 4 \mid d,\ 3 \mid d \end{cases}$$

for $1 \leq h \leq \omega(d) - \theta$. Further, from $\mathcal{X}k^2 > d \geq 2^{\delta}\mathfrak{p}_1 \cdots \mathfrak{p}_{\omega(d)-\delta'}$, we get

$$k > k_1 := \begin{cases} \sqrt{(2^{\delta}/\mathcal{X})\prod_{i=2}^{\omega(d)+1-\delta'} p_i} & \text{if } 3 \mid d, \\ \sqrt{(2^{\delta}/\mathcal{X})\prod_{i=3}^{\omega(d)+2-\delta'} p_i} & \text{if } 3 \nmid d. \end{cases}$$

Thus

(8.14) $$k > k_2 := \max(1733, k_1).$$

Further, we derive from (8.13) that

$$\frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_h - 1}{2} < \mathcal{X}_2^h := \begin{cases} \frac{1}{2^{h-1}}\left(\frac{\mathcal{X}k^2}{3\cdot 2^{\delta}}\right)^{(h-1)/(\omega(d)-1-\delta')} & \text{if } 3 \mid d, \\ \frac{1}{2^h}\left(\frac{\mathcal{X}k^2}{2^{\delta}}\right)^{h/(\omega(d)-\delta')} & \text{if } 3 \nmid d \end{cases}$$

for $1 \leq h \leq \omega(d) - \delta'$.

We take $r=[(\omega(d)-1)/2]$ if d is odd and $r=[\omega(d)/2]-1$ if d is even. By Corollary 3.8 and $|T_1|>0.42k$ by Lemma 4.3, we have

$$s_{r+1}\geq \frac{0.42k}{2^{\omega(d)-r-\theta}}-2\lambda_r-2^{r-1}\lambda_1-\sum_{\mu=2}^{r-1}2^{r-\mu}\lambda_\mu. \tag{8.15}$$

This with Corollary 4.5 and $\mathfrak{q}_1\cdots\mathfrak{q}_h<\mathcal{X}_1^h$ by (8.13) gives

$$s_{r+1}\geq\mathcal{X}_3:=\begin{cases}\dfrac{0.42k}{2^{\omega(d)-r}}-\dfrac{\mathcal{X}_1^r}{3\cdot 2^{r-3}}-\displaystyle\sum_{\mu=1}^{r-1}\frac{2^{r+2}}{3}\frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \text{if } 2\nmid d,\ 3\nmid d,\\[2ex] \dfrac{0.42k}{2^{\omega(d)-\theta-r}}-\dfrac{\mathcal{X}_1^r}{3\cdot 2^{r-4+\delta}}-2^{r-1}\left(\dfrac{\mathcal{X}_1}{2^\delta}+1\right)-\displaystyle\sum_{\mu=2}^{r-1}\frac{2^{r+3-\delta}}{3}\frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \\ & \text{if } 2\mid d,\ 3\nmid d,\\[2ex] \dfrac{0.42k}{2^{\omega(d)-\theta-r}}-\dfrac{\mathcal{X}_1^r}{9\cdot 2^{r-4+\delta'}}-2^{r-1}\left(\dfrac{\mathcal{X}_1}{3\cdot 2^\delta}+1\right)-\displaystyle\sum_{\mu=2}^{r-1}\frac{2^{r+3-\delta'}}{9}\frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \\ & \text{if } 3\mid d,\ 8\nmid d,\\[2ex] \dfrac{0.42k}{2^{\omega(d)-r}}-2\left(\dfrac{\mathcal{X}_1^r}{24}+1\right)-\displaystyle\sum_{\mu=1}^{r-1}2^{r-\mu}\left(\frac{\mathcal{X}_1^\mu}{24}+1\right) & \\ & \text{if } 8\mid d,\ 3\mid d,\ r\leq 3,\\[2ex] \dfrac{0.42k}{2^{\omega(d)-r}}-\dfrac{\mathcal{X}_1^r}{9\cdot 2^{r-3}}-\displaystyle\sum_{\mu=1}^{3}2^{r-\mu}\left(\frac{\mathcal{X}_1^\mu}{24}+1\right)-\sum_{\mu=4}^{r-1}\frac{2^{r+2}}{9}\frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \\ & \text{if } 8\mid d,\ 3\mid d,\ r\geq 4.\end{cases}$$

Observe that $(\mathcal{X}_3-\mathcal{X}_2^r)/k$ is an increasing function of k and is positive at $k=k_2$ except when $\omega(d)=7,\ d$ is odd and $3\mid d$, in which case it is positive at $k=11500$. Let $k\geq 25500$ when $\omega(d)=7,\ d$ is odd and $3\mid d$. Then

$$s_{r+1}\geq\mathcal{X}_3>\mathcal{X}_2^r>\frac{\mathfrak{p}_1-1}{2}\cdots\frac{\mathfrak{p}_r-1}{2}.$$

Therefore by Lemma 4.4 with $S=\{A_i : i\in T_{r+1}\},\ |S|=s_{r+1},\ h=r$ and by (8.13), we get

$$\mathcal{X}k^3>n+(k-1)d\geq\mathcal{X}_4k^2:=\begin{cases}\frac{3}{4}\cdot 2^{r+\delta}\mathcal{X}_3k^2 & \text{if } 3\nmid d,\\ \frac{9}{4}\cdot 2^{r+\delta-1}\mathcal{X}_3k^2 & \text{if } 3\mid d.\end{cases}$$

This is a contradiction by checking that $\mathcal{X}_4/k-\mathcal{X}>0$ except when d is odd, $3\mid d$ and $\omega(d)=6,8,9$. Thus we may assume that d is odd, $3\mid d$, $6\leq$

$\omega(d) \le 9$ and $k < 25500$ if $\omega(d) = 7$. Also, we check that $\mathcal{X}_4/k - \mathcal{X} > 0$ for $k = 5000, 62000, 350000$ according as $\omega(d) = 6, 8, 9$, respectively. Thus we may assume that $k < 5000, 25500, 62000, 350000$ whenever $\omega(d) = 6, 7, 8, 9$, respectively. If $\mathfrak{q}_1 \ge 7$, then we get a contradiction from $d < \mathcal{X}k^2 = \frac{1}{16}k^2$ and $d/7 \cdot 9 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \ge 1, 23, 23 \cdot 25, 23 \cdot 25 \cdot 29$ for $\omega(d) = 6, 7, 8, 9$, respectively. Thus $\mathfrak{q}_1 \in \{3, 5\}$. Further, we get $\mathfrak{q}_1 \le 5$, $\mathfrak{q}_2 \le 7$ if $\omega(d) = 6$; $\mathfrak{q}_1 \le 5$, $\mathfrak{q}_2 \le 7$, $\mathfrak{q}_3 \le 11$ if $\omega(d) = 7, 8$; and $\mathfrak{q}_1 = 3$, $\mathfrak{q}_2 = 5$, $\mathfrak{q}_3 = 7$ if $\omega(d) = 9$. Thus $\mathfrak{p}_1 = 3$ and $\mathfrak{p}_2 \in \{5, 7\}$ if $\omega(d) = 6$, and $\mathfrak{p}_2, \mathfrak{p}_3 \in \{5, 7, 11\}$ if $\omega(d) > 6$. Since $\left(\frac{a_i}{p}\right) = \left(\frac{n}{p}\right)$ for $p \,|\, d$, we consider Legendre symbols modulo $3, \mathfrak{q}_1, \mathfrak{q}_2$ for all squarefree positive integers $\le \mathfrak{q}_1$ and $\le \mathfrak{q}_1\mathfrak{q}_2$ to obtain $\lambda_1 \le 1, \lambda_2 \le 3$. Further, for $\omega(d) > 6$, we consider Legendre symbols modulo $3, \mathfrak{q}_1, \mathfrak{q}_2$ and $\mathfrak{q}_3$ if $\mathfrak{q}_3 \ne 9$ for all squarefree positive integers $\le \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ to get $\lambda_3 \le 17$. Therefore we deduce from (8.15) and Corollary 4.5 that

$$s_{r+1} \ge \mathcal{X}_5 := \begin{cases} \dfrac{0.42k}{2^4} - 8 & \text{if } \omega(d) = 6, \\ \dfrac{0.42k}{2^{\omega(d)-3}} - 44 & \text{if } \omega(d) = 7, 8, \\ \dfrac{0.42k}{2^5} - \dfrac{1}{9}\left(\dfrac{1}{16}\right)^{4/9} k^{8/9} - 54 & \text{if } \omega(d) = 9. \end{cases}$$

We check that

$$s_{r+1} \ge \mathcal{X}_5 > \mathcal{X}_2^r > \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_r - 1}{2}$$

by observing that $(\mathcal{X}_5 - \mathcal{X}_2^r)/k$ is an increasing function of k and is positive at $k = \max(1733, k_1)$. Therefore by Lemma 4.4 with $h = r$ and (8.13), we get $\frac{1}{16}k^3 > n + (k-1)d \ge \frac{9}{8} \cdot 2^r \mathcal{X}_5 k^2$. This is a contradiction since $\mathcal{X}_5/k - 1/(18 \cdot 2^r) > 0$.

Thus $|S_1| \ge \mathcal{X}_6$ using $|T_1| > 0.42k$ by Lemma 4.3, where $\mathcal{X}_6 = 0.42k - \mathfrak{h}(3) + 1$ if d is odd and $\mathcal{X}_6 = 0.42k - \mathfrak{h}(5) + 1$ if d is even. Since there exists a non-degenerate double pair, we apply Lemma 3.4 with $z_0 = 2$ to get a partition (d_1, d_2) of d with

$$\begin{cases} \mathfrak{p}_1 \cdots \mathfrak{p}_{[(\omega(d)+1)/2]} \le \max(d_1, d_2) < 4k & \text{if } 2 \nmid d, \\ \mathfrak{p}_1 \cdots \mathfrak{p}_{[\omega(d)/2]} \le \max(d_1, d_2) < 4k & \text{if } 2 \,\|\, d, \\ 2\mathfrak{p}_1 \cdots \mathfrak{p}_{[\omega(d)/2]} \le \max(d_1, d_2) < 8k & \text{if } 4 \,|\, d. \end{cases}$$

Let $\omega(d) \ge 7 + \delta'$. Then we see from (8.12) that

$$|S_1| \ge \mathcal{X}_6 > \frac{k}{4} > \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_4 - 1}{2}.$$

We now apply Lemma 4.4 with $h = 4$ to get $\mathcal{X}_0 k > n + (k-1)d \ge \frac{3}{4} \cdot 2^{4+\delta} \mathcal{X}_6 k^2 > 3 \cdot 2^\delta k^3$ since $\mathcal{X}_6 > k/4$. This contradicts (8.11). Thus $\omega(d) \le 6 + \delta'$ and $k \ge 1733$ by (8.12).

Assume that $k-|R|\ge \mathfrak{h}(3)$. Then from Corollary 3.10 with $z_0=3$, we get $n+(k-1)d<\mathcal{X}_7k^3$ where $\mathcal{X}_7=3/16$ if $2\parallel d$ and $3/4$ otherwise. If $2\mid d$ or $3\mid d$, then $n+(k-1)d\ge 3(\mathcal{X}_6-1)k^2$ if $3\mid d$ and $n+(k-1)d\ge 2^{\delta}(\mathcal{X}_6-1)k^2$ if $2\mid d$, contradicting $n+(k-1)d<\mathcal{X}_7k^3$. Thus d is odd, $3\nmid d$ and $\omega(d)=5,6$. By Corollary 3.10 with $z_0=3$, there is a partition (d_1,d_2) of d with $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\le\max(d_1,d_2)<2(k-1)$. Now we get

$$\frac{k}{4}>\frac{\mathfrak{p}_1-1}{2}\,\frac{\mathfrak{p}_2-1}{2}\,\frac{\mathfrak{p}_3-1}{2}.$$

Further, we check $\mathcal{X}_6>k/4$, implying

$$|S_1|\ge\mathcal{X}_6>\frac{\mathfrak{p}_1-1}{2}\,\frac{\mathfrak{p}_2-1}{2}\,\frac{\mathfrak{p}_3-1}{2}.$$

Therefore we derive from Lemma 4.4 with $h=3$ that $\frac{3}{4}k^3=\mathcal{X}_7k^3>n+(k-1)d\ge 6\mathcal{X}_6k^2>\frac{3}{2}k^3$, a contradiction. Hence $k-|R|<\mathfrak{h}(3)$. By Lemma 7.6(i)–(iv), we see that d is odd, $\omega(d)=6$ and $1733\le k<2082$. Further, from Lemma 7.6(v), (vi), we get $\mathfrak{p}_1\ge 11$. Now $11\cdot13\cdot17\cdot19\cdot23\cdot29\le d<3k^2$ by (8.10) and (8.11). This is a contradiction. ∎

Corollary 8.5. *Equation* (1.1) *with* $\omega(d)\ge 5$ *implies* $k-|R|<2^{\omega(d)-\theta}$.

Proof. Assume (1.1) with $\omega(d)\ge5$ and $k-|R|\ge 2^{\omega(d)-\theta}$. By Lemma 3.9, there exists a set Ω with at least $2^{\omega(d)-\theta}$ pairs having Property ND. Since there are at most $2^{\omega(d)-\theta}-1$ permissible partitions of d by Lemma 3.5(i), we can find a partition (d_1,d_2) of d and a non-degenerate double pair with respect to (d_1,d_2). This contradicts Lemma 8.4. ∎

Lemma 8.6. *Equation* (1.1) *with d odd*, $k\ge 101$ *and* $5\le\omega(d)\le 7$ *implies that* $k-|R|\le 2^{\omega(d)-1}$.

Proof. Let d be odd. Assume (1.1) with $5\le\omega(d)\le7$ and $k-|R|\ge 2^{\omega(d)-1}+1$. By Corollary 8.5, we may suppose that $k-|R|<2^{\omega(d)}$. Further, by Lemma 7.6(i), we obtain $k\le 555, 1056, 2099$ when $\omega(d)=5,6,7$, respectively. Since $k-|R|\ge 2^{\omega(d)-1}+1$, we derive from Corollary 3.11 that there exists a partition (d_1,d_2) of d such that $\mathfrak{D}_{12}:=\max(d_1,d_2)<(k-1)^2$.

Let $\omega(d)=5$. Then $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\le\mathfrak{D}_{12}<(k-1)^2$, implying $\mathfrak{p}_1\le 61$ since $67\cdot71\cdot73>555^2$. Also, $\mathfrak{p}_2<(k-1)/\sqrt{\mathfrak{p}_1}$. By taking $r=6$ for $208<k\le547$, we see from (6.10) and (6.13) with $p=\mathfrak{p}_1$ that $k-|R|\ge k-F'(k,r)+\min(-2^{r-2},\sigma_{61}-2^{r-1})\ge 32$ if $k>208$. Thus $k\le 208$. Further, $\mathfrak{p}_1\le 29$ since $31\cdot37\cdot41>208^2$. If $\mathfrak{p}_1\ge 17$, then we deduce from Lemma 7.5(a), (b) that $207^2>\mathfrak{D}_{12}\ge\min(17\cdot53\cdot59, 23\cdot47\cdot53)$, a contradiction. Therefore $\mathfrak{p}_1\le 13$ and hence $53\le\mathfrak{p}_2<k$ by Lemma 7.5(a). By taking $r=6$, we see from (6.14) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $g_{\mathfrak{p}_1,\mathfrak{p}_2}=2^{r-3}$ if $k\le127$ and $g_{\mathfrak{p}_1}=2^{r-2}$ if $k>127$ by (6.13) with $p=\mathfrak{p}_1$. From (6.10) and $\sigma_{\mathfrak{p}_2}\ge2$, we have $k-|R|\ge k-F'(k,r)+2-2^{r-3}$ if $k\le127$ and $k-|R|\ge k-F'(k,r)+2-2^{r-2}$ if $k>127$, which gives $k-|R|\ge 32$, a contradiction.

Let $\omega(d) = 6$. Then $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \le \mathfrak{D}_{12} < (k-1)^2$, implying $\mathfrak{p}_1 < \mathfrak{p}_2 \le 97$ since $101\cdot 103\cdot 107 > 1055^2$. By taking $r = 7$ for $384 < k \le 1039$, we get from (6.10) and (6.14) with $(p, q) = (\mathfrak{p}_1, \mathfrak{p}_2)$ that $k - |R| \ge k - F'(k, r) - 2^{r-2} \ge 64$ if $k > 384$. Thus $k \le 384$. Further, $\mathfrak{p}_2 \le 43$ since $47 \cdot 53 \cdot 59 > 383^2$. Then we derive from Lemma 7.5(a), (b) that $\mathfrak{p}_1 = 31$, $\mathfrak{p}_2 = 41$, $\mathfrak{p}_3 \ge 47$. Also, $k > 319$ since $41 \cdot 47 \cdot 53 > 319^2$. By taking $r = 7$ for $319 < k \le 384$, we deduce from (6.10) and (6.14) with $(p, q) = (31, 41)$ that $k - |R| \ge k - F'(k, r) + \sigma_{31} + \sigma_{41} - 2^{r-2} \ge 64$. This is a contradiction.

Let $\omega(d) = 7$. Suppose $\mathfrak{p}_1 \le 19$. By Lemma 7.6(v)–(vii), we get $k < 735, 930, 1200$ according as $\mathfrak{p}_1 = 3$, $\mathfrak{p}_1 \in \{5, 7\}$, $\mathfrak{p}_1 \ge 11$. By Lemma 7.5(a), we obtain $\mathfrak{p}_2 \ge 53$. Now $53 \cdot 59 \cdot 61 \le \mathfrak{D}_{12}/\mathfrak{p}_1 < 735^2/3, 930^2/5, 1200^2/11$ according as $\mathfrak{p}_1 = 3$, $\mathfrak{p}_1 \in \{5, 7\}$, $\mathfrak{p}_1 \ge 11$, respectively. This is not possible. Thus $\mathfrak{p}_1 \ge 23$. Further, $\mathfrak{p}_1 \le 41$, $\mathfrak{p}_2 \le 53$ from $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \le \mathfrak{D}_{12} < (k-1)^2 \le 2098^2$. By taking $r = 9$, we see from (6.10) and (6.14) with $(p, q) = (\mathfrak{p}_1, \mathfrak{p}_2)$ that $k - |R| \ge k - F'(k, r) + \min(-2^{r-3} + \sigma_{53}, -2^{r-2} + \sigma_{41} + \sigma_{53}) \ge 128$ for $k > 1007$. Therefore $k \le 1007$. Now $1007^2 > \mathfrak{D}_{12} \ge \min(23\cdot 47\cdot 53\cdot 59, 31\cdot 41\cdot 47\cdot 53)$ by Lemma 7.5(b). This is not possible. ∎

Corollary 8.7. *Assume* (1.1) *with* $\omega(d) \ge 5$. *Then* $k < 308, 556, 1057, 2870$ *and* $2(\omega(d) - \theta)2^{\omega(d)-\theta}$ *for* $\omega(d) = 5, 6, 7, 8$ *and* ≥ 9, *respectively. In particular*, $k < 2\omega(d)2^{\omega(d)}$.

Proof. By Corollary 8.5 and Lemma 8.6, we derive that $k - |R| < 2^{\omega(d)-\theta}$ and $k - |R| \le 2^{\omega(d)-1}$ if d is odd, $5 \le \omega(d) \le 7$. By Lemma 7.6(i), (ii), we get $k < 2(\omega(d) - \theta)2^{\omega(d)-\theta}$ for $\omega(d) \ge 9 + \theta$, $k < 4252$ if $\omega(d) = 8$ and $k < 308, 556, 1057$ according as $\omega(d) = 5, 6, 7$, respectively. Now it remains to consider $\omega(d) = 9$ if $2 \parallel d$, $4 \parallel d$ and $\omega(d) = 8$. By Lemma 7.6(ii), it suffices to consider d odd and $\omega(d) = 8$. Further, $k < 4252$ and $k - |R| < 256$. Suppose $k \ge 2870$. Then $k - |R| \ge 129$ by Lemma 7.6(i) and Corollary 3.11 yields a partition (d_1, d_2) of d with $\max(d_1, d_2) < (k-1)^2$. Let $\mathfrak{p}_1 \ge 53$. Then $4252^4 > d \ge 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83$, a contradiction. Thus $\mathfrak{p}_1 \le 47$. Now we deduce from Lemma 7.6(vi) that $k - |R| \ge 256$, a contradiction. ∎

Lemma 8.8.

(i) *Let d be odd and $\omega(d) = 5, 6$. Suppose that d is divisible by a prime $\le k$ when $\omega(d) = 5$. Further, assume that there exist distinct primes p and q with $pq \mid d$, $p \le 19, q \le k$ when $\omega(d) = 6$. Then* (1.1) *with $k \ge 101$ has no solution.*

(ii) *Let d be even and $5 \le \omega(d) \le 6 + \theta$. Assume that $p \mid d$ with $p \le 47$ when $\omega(d) = 7$. Then* (1.1) *with $k \ge 101$ has no solution.*

Proof. By Corollary 8.5, we may suppose that $k - |R| < 2^{\omega(d)-\theta}$.

(i) Let d be odd. From Corollary 8.7, we get $k < 308, 556$ when $\omega(d) = 5, 6$, respectively. Let $\omega(d) = 5$. By taking $r = 5$ for $101 \le k < 308$, we find from (6.10) and (6.13) with $p=\mathfrak{p}_1$ that $k-|R|\ge k-F'(k,r)-2^{r-1}\ge 17$, which is not possible by Lemma 8.6.

Let $\omega(d)=6$. Then $53\le\mathfrak{p}_2\le k$ by Lemma 7.5(a). We take $r=6$. Let $\mathfrak{p}_1\le 13$. Then we see from (6.14) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $g_{\mathfrak{p}_1,\mathfrak{p}_2}=2^{r-3}$ if $k\le 127$ and $g_{\mathfrak{p}_1}=2^{r-2}$ if $k>127$ by (6.13) with $p=\mathfrak{p}_1$. From (6.10) and $\sigma_{\mathfrak{p}_2}\ge 1$, we have $k-|R|\ge k-F'(k,r)+1-2^{r-3}$ if $k\le 127$ and $k-|R|\ge k-F'(k,r)+1-2^{r-2}$ if $k>127$, giving $k-|R|\ge 33$. This contradicts Lemma 8.6. Thus $\mathfrak{p}_1\in\{17,19\}$. We find from (6.14) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $g_{\mathfrak{p}_1,\mathfrak{p}_2}=2^{r-2}$ if $k\le 193$ and $g_{\mathfrak{p}_1}=2^{r-1}$ if $k>193$ by (6.13) with $p=\mathfrak{p}_1$. From (6.10) and $\sigma_{\mathfrak{p}_1}+\sigma_{\mathfrak{p}_2}\ge\sigma_{19}+1$, we get $k-|R|\ge 33$, a contradiction.

(ii) Let d be even. Then from Lemma 7.6(ii)–(iv), we get $\omega(d)=6$, $k<252$ and $\omega(d)=7$, $k<430$ if $2\,\|\,d$; $\omega(d)=6$, $k<127$ and $\omega(d)=7$, $k<303$ if $4\,\|\,d$; $\omega(d)=6$, $k<220$ if $8\mid d$. By Lemma 7.5, we obtain $\omega(d)=6$, $k<252$ and $\mathfrak{p}_1\ge 53$. Further, by Lemma 7.6, we get $k-|R|\ge 2^{\omega(d)-\theta-1}+1$. This with Corollary 3.11 gives $\max(d_1,d_2)<(k-1)^2$ for some partition (d_1,d_2) of d. Since $\max(d_1,d_2)\ge\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\ge 53^3>430^2$, we get a contradiction. ∎

LEMMA 8.9. *Equation* (1.1) *with* $k\ge 101$ *implies that* $d>10^{10}$.

Proof. Assume (1.1) with $k\ge 101$ and $d\le 10^{10}$. By Lemma 8.2, we have $\omega(d)\ge 5$. Further, we deduce from Corollary 8.5 that $k-|R|<2^{\omega(d)-\theta}$, which we use without reference in the proof.

Let d be odd. Then $\omega(d)\le 9$, otherwise $d\ge\prod_{i=2}^{11}p_i>10^{10}$. By Lemma 8.8(i), we see that $d>k^5>10^{10}$ if $\omega(d)=5$. Thus $\omega(d)\ge 6$.

Let $\omega(d)=6$. If $\mathfrak{p}_1\le 19$, then $d>k^5>10^{10}$ by Lemma 8.8(i). Therefore $\mathfrak{p}_1\ge 23$. Also, $\mathfrak{p}_1\le 37$, otherwise $d\ge 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61>10^{10}$. Further, $k<556$ by Corollary 8.7. Therefore by Lemma 7.5(b), we obtain $d\ge\min(23\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67, 31\cdot 41\cdot 47\cdot 53\cdot 59\cdot 61)>10^{10}$.

Thus $\omega(d)\ge 7$. Then $\mathfrak{p}_1\le 13$, otherwise $d\ge\prod_{i=7}^{13}p_i>10^{10}$. Further, $k\ge 1733$, otherwise $d\ge 3\cdot 53^6>10^{10}$ by Lemma 7.5(a). By Corollary 8.7, we obtain $\omega(d)\ge 8$.

Let $\omega(d)=8$. Then $\mathfrak{p}_1\le 7$. Now Lemma 7.6(v), (vi) gives $\mathfrak{p}_1\in\{5,7\}$. Further, $\mathfrak{p}_2\le 11$ since $5\prod_{i=6}^{12}p_i>10^{10}$. This is not possible by Lemma 7.6(vii) since $k\ge 1733$.

Let $\omega(d)=9$. Then $\mathfrak{p}_1=3$, $\mathfrak{p}_2=5$ and $\mathfrak{p}_3=7$. This is not possible by Lemma 7.6(vii) since $k\ge 1733$.

Let d be even. Then $\omega(d)\le 10$, otherwise $d\ge\prod_{i=1}^{11}p_i>10^{10}$. Further, $\omega(d)\le 9$ for $4\mid d$ since $4\prod_{i=2}^{10}p_i>10^{10}$. By Lemma 8.8(ii), we have $\omega(d)\ge 7$. Further, $k\ge 1801$ by Lemma 7.5(c) since $2\prod_{i=16}^{21}p_i>10^{10}$. Now we use Lemma 7.6(ii)–(iv) to obtain either $2\,\|\,d,\omega(d)=9,10$ or $8\mid d$, $\omega(d)=9$.

Let $2\,\|\,d$. Let $\omega(d)=9$. Then $\mathfrak{p}_1\le 5$, otherwise $d\ge 2\prod_{i=4}^{11}p_i>10^{10}$. Then $k-|R|\ge 256$ by Lemma 7.6(vii), a contradiction. Let $\omega(d)=10$.

Then $\mathfrak{p}_1 = 3$, $\mathfrak{p}_2 = 5$ and hence $k - |R| \geq 512$ by Lemma 7.6(vii). This is not possible.

Let $8 \mid d$ and $\omega(d) = 9$. Then $\mathfrak{p}_1 \leq 5$ since $8\prod_{i=4}^{11} p_i > 10^{10}$. By Lemma 7.6, we get $k - |R| \geq 512$, which is a contradiction. ∎

9. Proof of Theorem 2. Suppose that (1.1) with $b = 1$ has a solution. By Theorem $\mathcal{A}$(b), Lemmas 8.2, 8.6 and Corollary 8.7, we see that $\omega(d) = 5$, d is odd, $k-|R| \leq 16$ and $110 \leq k < 308$. We observe that $\mathrm{ord}_p(a_0a_1\cdots a_{k-1})$ is even for each prime p. Therefore the number of i's for which a_i's are divisible by p is at most $\sigma'_p = \lceil k/p \rceil$ or $\lceil k/p \rceil - 1$ according as $\lceil k/p \rceil$ is even or odd. Let $r = 4$. Then from (6.3), we get

$$k - |R| \geq k - F(k, r) - 2^r \geq k - \sum_{p>p_r} \sigma'_p - 2^r,$$

which is ≥ 17 except at $k = 110, 112, 114, 116, 118, 120, 122, 124$ where $k - |R| \geq 16$. Hence $k = 110, 112, 114, 116, 118, 120, 122, 124$ and $k - |R| = 16$. Further, we may assume that for each prime $11 \leq p \leq k$, there are exactly σ'_p many i's for which $p \mid a_i$, and for any i, $pq \nmid a_i$ whenever $11 \leq q \leq k$, $q \neq p$. Consider the i's for which a_i's are divisible by primes $109, 107$ when $k = 110$; $37, 109, 107$ when $k = 112$; $113, 37, 109, 107$ when $k = 114$; $23, 113, 37, 109, 107$ when $k = 116$; $13, 23, 113, 37, 109, 107$ when $k = 118$; $17, 13, 23, 113, 37, 109, 107$ when $k = 120$; $11, 17, 13, 23, 113, 37, 109, 107$ when $k = 122$; and $41, 11, 17, 13, 23, 113, 37, 109, 107$ when $k = 124$. Then $P(a_{\varsigma_k}a_{\varsigma_k+1}\cdots a_{\varsigma_k+105}) \leq 103$ where $\varsigma_k = 2 + (k - 110)/2$. This is excluded. For instance, let $k = 124$. Then $P(a_9a_{10}\cdots a_{114}) \leq 103$. This gives $103^2 \mid a_ja_{j+103}$ for $j \in \{9, 10, 11\}$. Let $103^2 \mid a_9a_{112}$. Then $101^2 \mid a_ja_{j+101}$ for $j \in \{10, 12, 13\}$ so that $P(a_{14}a_{15}\cdots a_{110}) \leq 97$. This is excluded by considering Theorem $\mathcal{A}$ with $k = 97$. If $103^2 \mid a_1a_{114}$, we obtain similarly $P(a_{13}a_{14}\cdots a_{109}) \leq 97$ and this is excluded. Thus $103^2 \mid a_{10}a_{113}$. If $101^2 \mid a_ja_{j+101}$ for $j \in \{11, 13\}$, we get $P(a_{14}a_{15}\cdots a_{110}) \leq 97$ and this is excluded. Hence $101^2 \mid a_9a_{110}$ this implying $P(a_{11}a_{12}\cdots a_{107}) \leq 97$, and this is excluded again. ∎

10. Proof of Theorem 3. By Theorem $\mathcal{A}$(a) and Lemmas 8.2, 8.8(ii), we may suppose that d is odd, either $\omega(d) = 3$, $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}_2$ or $\omega(d) \leq 2$, $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}_1 \cup \mathfrak{S}_2$, $(a_0, a_1, \ldots, a_7)$ is not $(3, 1, 5, 6, 7, 2, 1, 10)$ or its mirror image when $k = 8$, $\omega(d) = 2$. For $p \mid d$, we observe from $\left(\frac{q}{p}\right) = 1$ for $q \in \{2, 3, 5, 7\}$ that $p \geq 311$ and therefore $d \geq 311^{\omega(d)}$. Further, we observe from Lemma 4.2 that (3.24) is valid.

Let $\omega(d) = 1$. If $k - |R| \geq 2$, we get $d = d_2 < 4(k - 1)$ by Corollary 3.10 with $z_0 = 2$, a contradiction since $d \geq 311$. Therefore it remains to consider $k = 8$ and $(a_0, \ldots, a_7) = (3, 1, 5, 6, 7, 2, 1, 10)$ or its mirror image.

We exclude the possibility $(a_0, \ldots, a_7) = (3,1,5,6,7,2,1,10)$; the proof for its mirror image is similar. We write

$$n = 3x_0^2, \quad n+d = x_1^2, \quad n+2d = 5x_2^2, \quad n+3d = 6x_3^2,$$
$$n+4d = 7x_4^2, \quad n+5d = 2x_5^2, \quad n+6d = x_6^2, \quad n+7d = 10x_7^2.$$

Then we get $5d = x_6^2 - x_1^2 = (x_6 - x_1)(x_6 + x_1)$, implying either $x_6 - x_1 = 1$, $x_6 + x_1 = 5d$ or $x_6 - x_1 = 5, x_6 + x_1 = d$. We apply Runge's method to arrive at a contradiction. Suppose $x_6 - x_1 = 1, x_6 + x_1 = 5d$. Then $5d = 2x_1 + 1$ and $x_1 \geq 14$. We obtain $(125 \cdot 6x_0x_3x_5)^2 = (25(n+d) - 25d)(25(n+d) + 50d)(25(n+d) + 100d) = (25x_1^2 - 10x_1 - 5)(25x_1^2 + 20x_1 + 10)(25x_1^2 + 40x_1 + 20) = 15625x_1^6 + 31250x_1^5 + 20625x_1^4 - 3000x_1^3 - 10750x_1^2 - 6000x_1 - 1000 =: \psi(x_1)$. We see that

$$(125x_1^3 + 125x_1^2 + 20x_1 - 32)^2 > \psi(x_1) > (125x_1^3 + 125x_1^2 + 20x_1 - 33)^2.$$

This is a contradiction. Let $x_6 - x_1 = 5, x_6 + x_1 = d$. Then we argue as above to conclude that $d = 2x_1 + 5, x_1 \geq 66$ and

$$(x_1^3 + 5x_1^2 + 4x_1 - 32)^2 > \psi_1(x_1) > (x_1^3 + 5x_1^2 + 4x_1 - 33)^2,$$

where $\psi_1(x_1) = x_1^6 + 10x_1^5 + 33x_1^4 - 24x_1^3 - 430x_1^2 - 1200x_1 - 1000$ is a square. This is again not possible.

Thus $\omega(d) \geq 2$. Let $k \geq 13$ and $(a_0, a_1, \ldots, a_{12}) \neq (3,1,5,6,7,2,1,10,11,3,13,14,15)$ or its mirror image when $k = 13$. Let $\mathfrak{g} = 3,4,5$ if $k = 13, 14$, $k \geq 19$, respectively. Then from $\nu(1) = 3$ and Lemma 3.9, we get a set Ω of pairs (i,j) with $|\Omega| \geq k - |R| + r_3 \geq \mathfrak{g}$ having Property ND. Therefore there exists a non-degenerate double pair for $k \geq 14$ when $\omega(d) = 2$. Further, there are distinct pairs corresponding to partitions (d_1, d_2), (d_2, d_1) for some divisor d_1 of d for $k \geq 13$ when $\omega(d) = 2$ and for $k \geq 19$ when $\omega(d) = 3$.

Suppose that there is a non-degenerate double pair. Then we see from Lemma 3.4 with $z_0 = 2$ that $d < 3k^2 \leq 3 \cdot 24^2$, contradicting $d \geq 311^2$. Thus there is no non-degenerate double pair corresponding to any partition. Again, if there are pairs $(i,j), (g,h)$ corresponding to partitions $(d_1, d_2), (d_2, d_1)$ for some divisor d_1 of d, then we derive from Lemma 3.3 that $d < (k-1)^4$. This is not possible since $311^2 \leq d < 12^4$ when $\omega(d) = 2$ and $311^3 \leq d < 23^4$ when $\omega(d) = 3$. Therefore there are no distinct pairs corresponding to partitions $(d_1, d_2), (d_2, d_1)$ for any divisor d_1 of d. Thus it remains to consider $k = 14$ when $\omega(d) = 3$ and either $k = 8, 9$ or $k = 13$, $(a_0, a_1, \ldots, a_{12}) = (3,1,5,6,7,2,1,10,11,3,13,14,15)$ or its mirror image when $\omega(d) = 2$. Also, we may suppose that there is a pair (i,j) with $a_i = a_j$ corresponding to the partition $(1,d)$ for each of these possibilities.

Let $k = 8$ and $\omega(d) = 2$. We exclude the possibility $(a_0, a_1, \ldots, a_7) = (2,3,1,5,6,7,2,1)$; the proof for its mirror image is similar. We see that either $(0,6)$ or $(2,7)$ corresponds to $(1,d)$ and we arrive at a contradiction as in the case $k = 8$, $\omega(d) = 1$ and $(a_0, \ldots, a_7) = (3,1,5,6,7,2,1,10)$. Let $(0,6)$ correspond to $(1,d)$. Then either $x_6 - x_0 = 1$, $x_6 + x_0 = 3d$ or $x_6 - x_0 = 3$, $x_6 + x_0 = d$. Suppose $x_6 - x_0 = 1$, $x_6 + x_0 = 3d$. Then we obtain $3d = 2x_0 + 1$, $x_0 \geq 100$ and $(3x_2x_7)^2 = (3n+6d)(3n+21d) = (6x_0^2 + 4x_0 + 2) \cdot (6x_0^2 + 14x_0 + 7) = 36x_0^4 + 108x_0^3 + 110x_0^2 + 56x_0 + 14 =: \psi_2(x_0)$ is a square. This is a contradiction since $(6x_0^2 + 9x_0 + 3)^2 > \psi_2(x_0) > (6x_0^2 + 9x_0 + 2)^2$. Let $x_6 - x_0 = 3$, $x_6 + x_0 = d$. Then we argue as above to conclude that $d = 2x_0 + 3$, $x_0 \geq 100$ and $4x_0^4 + 36x_0^3 + 11x_0^2 + 168x_0 + 126 =: \psi_3(x_0)$ is a square. This is again not possible since $(2x_0^2 + 9x_0 + 8)^2 > \psi_3(x_0) > (2x_0^2 + 9x_0 + 7)^2$. The other possibility, of $(2,7)$ corresponding to $(1,d)$, is excluded similarly.

Let $k = 9$ and $\omega(d) = 2$. Then (1.1) holds with $k = 8$ and $(a_0, \ldots, a_7) = (2,3,1,5,6,7,2,1)$ or its mirror image. This is already excluded. The case $k = 13, \omega(d) = 2$ and $(a_0, \ldots, a_{12}) = (3,1,5,6,7,2,1,10,11,3,13,14,15)$ or its mirror image is excluded as above in the case $k = 8$.

Let $k = 14$ and $\omega(d) = 3$. Let $(a_0, \ldots, a_{13}) = (3,1,5,6,7,2,1,10,11,3,13, 14,15,1)$. Then one of the pairs $(0,9), (1,6), (1,13), (6,13)$ corresponds to the partition $(1,d)$. This is excluded as above in the case $k = 8, \omega(d) = 2$. The proof for the mirror image $(1,15,14,13,3,11,10,1,2,7,6,5,1,3)$ is similar. ∎

11. Proof of Theorem 1. First we show that $d > 10^{10}$. By Lemma 8.9 and Theorem $\mathcal{A}$(a), it suffices to consider the case $k = 7$ and $(a_0, a_1, \ldots, a_6)$ given by

$$(2,3,1,5,6,7,2),\ (3,1,5,6,7,2,1),\ (1,5,6,7,2,1,10) \tag{11.1}$$

or their mirror images. Then for $p \mid d$, we have $\left(\frac{q}{p}\right) = 1$ for $q \in \{2,3,5,7\}$. Suppose that $d \leq 10^{10}$. Since $\omega(d) \geq 2$, we have $\mathfrak{p}_1 \leq 10^5$. For $X > 0$, let

$$\mathcal{P}_0 = \mathcal{P}_0(X) = \left\{ p \leq X : \left(\frac{q}{p}\right) = 1,\ q = 2,3,5,7 \right\}.$$

We find that $\mathcal{P}_0(10^5) = \{311, 479, 719, 839, 1009, \ldots\}$. Thus $\mathfrak{p}_1 \geq 311$ by $\mathfrak{p}_1 \in \mathcal{P}_0(10^5)$. Since $311 \cdot 479 \cdot 719 \cdot 839 > 10^{10}$, we have $\omega(d) \leq 3$. Further, from $311^2 \cdot 479^2 > 10^{10}$, we get either $\omega(d) = 2$, $d = \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1^2\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2^2$ or $\omega(d) = 3$, $d = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Consider $(a_0, a_1, \ldots, a_6) = (2,3,1,5,6,7,2)$. From $d = n + d - n = 3x_1^2 - 2x_0^2$, $3 \nmid x_0$, $4 \nmid x_0x_1$, we get $d \equiv -2 \equiv 1 \pmod 3$ and $d \equiv 3 - 2 \equiv 1 \pmod 8$, giving $d \equiv 1 \pmod{24}$. Again, from $2(x_6^2 - x_0^2) = n + 6d - n = 6d = 6d_1d_2$, we get $x_6 - x_0 = r_1d_1$, $x_6 + x_0 = r_2d_2$ with $r_1r_2 = 3$, $r_1d_1 < r_2d_2$ and $(r_1d_1, r_2d_2) \in \mathfrak{D}_3$ with

$$\mathfrak{D}_3 = \begin{cases} \{(1, 3\mathfrak{q}_1\mathfrak{q}_2), (3, \mathfrak{q}_1\mathfrak{q}_2), (\mathfrak{q}_1, 3\mathfrak{q}_2), (3\mathfrak{q}_1, \mathfrak{q}_2), (\mathfrak{q}_2, 3\mathfrak{q}_1)\} & \text{if } \omega(d) = 2, \\ \{(1, 3\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3), (3, \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3), (\mathfrak{p}_1, 3\mathfrak{p}_2\mathfrak{p}_3), (3\mathfrak{p}_1, \mathfrak{p}_2\mathfrak{p}_3), & \\ \quad (\mathfrak{p}_2, 3\mathfrak{p}_1\mathfrak{p}_3), (3\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_3), (\mathfrak{p}_3, 3\mathfrak{p}_1\mathfrak{p}_2), (3\mathfrak{p}_3, \mathfrak{p}_1\mathfrak{p}_2)\} & \text{if } \omega(d) = 3. \end{cases}$$

Then $x_0=(r_2d_2-r_1d_1)/2$, giving $x_2^2=n+2d=2x_0^2+2d_1d_2=\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2-2d_1d_2\}$ a square. Now we see from $3x_1^2=n+d=2x_0^2+d=\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2-4d_1d_2\}$ that $\frac{1}{6}\{(r_1d_1)^2+(r_2d_2)^2-4d_1d_2\}$ is a square. For each $d=\mathfrak{q}_1\mathfrak{q}_2$, we first check for $d\equiv 1\pmod{24}$ and restrict to such d. Further, for each possibility of $(r_1d_1,r_2d_2)\in\mathfrak{D}_3$ with $r_1d_1<r_2d_2$, we check whether $\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2-2d_1d_2\}$ is a square and restrict to such pairs (r_1d_1,r_2d_2). Finally, we check that $\frac{1}{6}\{(r_1d_1)^2+(r_2d_2)^2-4d_1d_2\}$ is not a square. For example, let $d=1319\cdot 4919$. Then $\mathfrak{q}_1=1319$, $\mathfrak{q}_2=4919$. We check that $d\equiv 1\pmod{24}$. For each choice $(r_1d_1,r_2d_2)\in\mathfrak{D}_3$ with $r_1d_1<r_2d_2$, we check whether $\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2-2d_1d_2\}$ is a square, which is possible only for $(r_1d_1,r_2d_2)=(1319,3\cdot 4919)$. However, we find that $\frac{1}{6}\{(r_1d_1)^2+(r_2d_2)^2-4d_1d_2\}$ is not a square for $(r_1d_1,r_2d_2)=(1319,3\cdot 4919)$.

Next we consider $(a_0,a_1,\dots,a_6)=(3,1,5,6,7,2,1)$. From $d=n+6d-(n+5d)=x_6^2-2x_5^2$, $3\nmid x_5$, $3\mid x_6^2$ and $2\nmid x_6$, $4\mid x_5^2$, we get $d\equiv 1\pmod{24}$. Again, from $x_6^2-x_1^2=n+6d-(n+d)=5d=5d_1d_2$ we get $x_6-x_1=r_1d_1$, $x_6+x_1=r_2d_2$ with $r_1r_2=5$, $r_1d_1<r_2d_2$ and

$$\mathfrak{D}_5=\begin{cases}\{(1,5\mathfrak{q}_1\mathfrak{q}_2),(5,\mathfrak{q}_1\mathfrak{q}_2),(\mathfrak{q}_1,5\mathfrak{q}_2),(5\mathfrak{q}_1,\mathfrak{q}_2),(\mathfrak{q}_2,5\mathfrak{q}_1)\} & \text{if } \omega(d)=2,\\ \{(1,5\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3),(5,\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3),(\mathfrak{p}_1,5\mathfrak{p}_2\mathfrak{p}_3),(5\mathfrak{p}_1,\mathfrak{p}_2\mathfrak{p}_3), & \\ \quad(\mathfrak{p}_2,5\mathfrak{p}_1\mathfrak{p}_3),(5\mathfrak{p}_2,\mathfrak{p}_1\mathfrak{p}_3),(\mathfrak{p}_3,5\mathfrak{p}_1\mathfrak{p}_2),(5\mathfrak{p}_3,\mathfrak{p}_1\mathfrak{p}_2)\} & \text{if } \omega(d)=3.\end{cases}$$

Thus $x_6=(r_2d_2+r_1d_1)/2$, giving $2x_5^2=n+5d=x_6^2-d=\frac{1}{4}\{(r_1d_1)^2+(r_2d_2)^2+6d\}$, whence $\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2+6d\}$ is a square. Further, from $7x_4^2=n+4d=n+6d-2d=x_6^2-2d=\frac{1}{4}\{(r_1d_1)^2+(r_2d_2)^2+2d_1d_2\}$, we find that $\frac{1}{7}\{(r_1d_1)^2+(r_2d_2)^2+2d_1d_2\}$ is a square. For each $d=\mathfrak{q}_1\mathfrak{q}_2$, we first check if $d\equiv 1\pmod{24}$ and restrict to such d. Further, for each possibility of $(r_1d_1,r_2d_2)\in\mathfrak{D}_5$ with $r_1d_1<r_2d_2$, we check whether $\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2+6d\}$ is a square and restrict to such pairs (r_1d_1,r_2d_2). Finally, we check that $\frac{1}{7}\{(r_1d_1)^2+(r_2d_2)^2+2d\}$ is not a square. Further, the case $(a_0,a_1,\dots,a_6)=(1,5,6,7,2,1,10)$ is excluded by the preceding test.

The case $(a_0,a_1,\dots,a_6)=(2,7,6,5,1,3,2)$ is similar to $(a_0,a_1,\dots,a_6)=(2,3,1,5,6,7,2)$; we obtain $d\equiv -1\pmod{24}$, and $\frac{1}{2}\{(r_1d_1)^2+(r_2d_2)^2+2d\}$ and $\frac{1}{6}\{(r_1d_1)^2+(r_2d_2)^2+4d\}$ are squares for each possibility of $(r_1d_1,r_2d_2)\in\mathfrak{D}_3$ with $r_1d_1<r_2d_2$. This is excluded. The cases $(a_0,a_1,\dots,a_6)=(1,2,7,6,5,1,3),(10,1,2,7,6,5,1)$ are also similar to that of $(a_0,a_1,\dots,a_6)=(3,1,5,6,7,2,1),(1,5,6,7,2,1,10)$ and are excluded. Thus $d>10^{10}$.

Now we show that $d>k^{\log\log k}$. Since $k^{\log\log k}<10^{10}$ for $k<22027$, we may assume that $k\ge 22027$. By Corollary 8.7, we obtain $\omega(d)\ge 9$ and $k<2(\omega(d)-\theta)2^{\omega(d)-\theta}=:\Psi_0(\omega(d)-\theta)$. Further, we derive from $22027\le k<2\omega(d)2^{\omega(d)}$ that $\omega(d)\ge 11$. It suffices to show that $\log d>(\log\Psi_0(\omega(d)-\theta))\cdot(\log\log\Psi_0(\omega(d)-\theta))=:\Psi_1(\omega(d)-\theta)$. Let $\Psi_2(l)=l(\log l+\log\log l-1.076868)$ for $l>1$. From $d\ge 2^{\delta}\prod_{i=2}^{\omega(d)+1-\delta'}p_i$ and Lemma 5.1(iv), we get $\log d>$

$\Psi_2(\omega(d)+1)-\log 2$, $\Psi_2(\omega(d))+(\delta-1)\log 2$ when $2\nmid d$, $2\mid d$, respectively. It suffices to check for $\omega(d)\geq 11$ that $\Psi_2(\omega(d)+1)-\log 2-\Psi_1(\omega(d))>0$ if $2\nmid d$, $\Psi_2(\omega(d))-\Psi_1(\omega(d)-1)>0$ if $2\parallel d$, $4\parallel d$ and $\Psi_2(\omega(d))+\log 4-\Psi_1(\omega(d))>0$ if $8\mid d$. This is indeed the case. ∎

12. Theorem 2 with $\omega(d)=2$ and $\gcd(n,d)\geq 1$. As stated in Section 1, we prove

THEOREM 4. *A product of eight or more terms in arithmetic progression with common difference d satisfying $\omega(d)=2$ is not a square.*

Proof. Suppose Theorem 4 is not true. Then (1.1) is valid with $k\geq 8$, $b=1$ and $\omega(d)=2$ but n and d not necessarily coprime. Let $n'=n/\gcd(n,d)$ and $d'=d/\gcd(n,d)$. Now, by dividing both sides of (1.1) by $\gcd(n,d)^k$, we have

$$n'(n'+d')\cdots(n'+(k-1)d')=\mathfrak{p}_1^{\delta_1}\mathfrak{p}_2^{\delta_2}y_1^2 \tag{12.1}$$

where $y_1>0$ is an integer and $\delta_1,\delta_2\in\{0,1\}$. We may assume that k is odd and $(\delta_1,\delta_2)\neq(0,0)$ by Theorem 2 with $\omega(d)=2$. Let $d'=1$. Then we see from [SaSh03b, Corollary 3] that the left hand side of (12.1) is divisible by at least three primes $>k$. Therefore there exists a prime p with $p\neq\mathfrak{p}_1$, $p\neq\mathfrak{p}_2$, $p>k$ such that it divides a term on the left hand side of (12.1) to a power at least 2. This implies $n'>k^2$. Now we see from [MuSh04b, Theorem 2] that the left hand side of (12.1) is divisible by at least three primes $>k$ to odd powers. This contradicts (12.1). Thus $d'>1$, implying $(\delta_1,\delta_2)\neq(1,1)$ by $\gcd(n',d')=1$. Now we may assume that $(\delta_1,\delta_2)=(1,0)$. Then d' is a power of $\mathfrak{p}_2$. Further, we may suppose that $\mathfrak{p}_1\geq k$ by the results stated in Section 1. Let $n+i_0d$ with $0\leq i_0<k$ be the term divisible by $\mathfrak{p}_1$ on the left hand side of (12.1). Then

$$n'\cdots(n'+(i_0-1)d')(n'+(i_0+1)d')\cdots(n'+(k-1)d')=b'y_2^2$$

where $P(b')<k$ and $y_2>0$ is an integer. Now $k=8$ by [MuSh04a, Theorem 1]. This is not possible since k is odd. ∎

References

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

[Dus98] P. Dusart, *Autour de la fonction qui compte le nombre de nombres premiers*, Ph.D. thesis, Univ. de Limoges, 1998.

[Dus99] —, *Inégalités explicites pour $\psi(X),\theta(X),\pi(X)$ et les nombres premiers*, C. R. Math. Acad. Sci. Soc. R. Can. 21 (1999), 53–59.

[ErSe75] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. 19 (1975), 292–301.

[FiHa01] P. Filakovszky and L. Hajdu, *The resolution of the diophantine equation* $x(x+d)\cdots(x+(k-1)d) = by^2$ *for fixed* d, Acta Arith. 98 (2001), 151–154.

[HLST07] N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman, *An extension of a theorem of Euler*, ibid. 129 (2007), 71–102.

[Lai06] S. Laishram, *An estimate for the length of an arithmetic progression the product of whose terms is almost square*, Publ. Math. Debrecen 68 (2006), 451–475.

[LaSh04] S. Laishram and T. N. Shorey, *Number of prime divisors in a product of terms of an arithmetic progression*, Indag. Math. 15 (2004), 505–521.

[LaSh06] —, —, *The greatest prime divisor of a product of terms in an arithmetic progression*, ibid. 17 (2006), 425–436.

[Mar85] R. Marszałek, *On the product of consecutive elements of an arithmetic progression*, Monatsh. Math. 100 (1985), 215–222.

[MuSh03] A. Mukhopadhyay and T. N. Shorey, *Almost squares in arithmetic progression (II)*, Acta Arith. 110 (2003), 1–14.

[MuSh04a] —, —, *Almost squares in arithmetic progression (III)*, Indag. Math. 15 (2004), 523–533.

[MuSh04b] —, —, *Square free part of products of consecutive integers*, Publ. Math. Debrecen 64 (2004), 79–99.

[Rob55] H. Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly 62 (1955), 26–29.

[Rob83] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith. 42 (1983), 367–389.

[RoSc62] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[Sar97] N. Saradha, *On perfect powers in products with terms from arithmetic progressions*, Acta Arith. 82 (1997), 147–172.

[SaSh03a] N. Saradha and T. N. Shorey, *Almost squares in arithmetic progression*, Compos. Math. 138 (2003), 73–111.

[SaSh03b] —, —, *Almost squares and factorisations in consecutive integers*, ibid. 138 (2003), 113–124.

[SaSh05] —, —, *Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression*, ibid. 141 (2005), 541–560.

[Sho02] T. N. Shorey, *Powers in arithmetic progression*, in: A Panorama in Number Theory or The View from Baker's Garden, G. Wüstholz (ed.), Cambridge Univ. Press, 2002, 325–336.

[ShTi90] 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: shanta@math.tifr.res.in
shorey@math.tifr.res.in

Received on 5.12.2006
and in revised form on 13.4.2007 (5340)