ACTA ARITHMETICA
134.4 (2008)

Squares in arithmetic progression with at most two terms omitted

by

Shanta Laishram (Waterloo, Ont.) 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 $\omega(1) = 0$. Let p_i be the ith prime number. Let $k \geq 4$, $t \geq k - 2$ and $\gamma_1 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Thus $t \in \{k, k-1, k-2\}$, $\gamma_t \geq k - 3$ and $\gamma_i = i - 1$ for $1 \leq i \leq t$ if $t = k$. We put $\psi = k - t$. Let b be a positive squarefree integer; we shall always assume, unless otherwise specified, that $P(b) \leq k$. We consider the equation

$$\Delta = \Delta(n, d, k) = (n + \gamma_1 d) \cdots (n + \gamma_t d) = by^2 \tag{1.1}$$

in positive integers n, d, k, b, y, t. We prove

Theorem 1. *Let $\psi = 2$, $k \geq 15$ and $d \nmid n$. Then* (1.1) *with $\omega(d) = 1$ does not hold.*

Let $\psi = 0$. 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]. Let $d > 1$. We observe that (1.1) has infinitely many solutions if $k = 2, 3$ and $b = 1$. Also (1.1) with $k = 4$ and $b = 6$ has infinitely many solutions. It has been conjectured that (1.1) with $\gcd(n, d) = 1$ and $k \geq 5$ does not hold. Let $\omega(d) = 1$. It has been shown in [SaSh03a] for $k > 29$ and [MuSh03] for $4 \leq k \leq 29$ that (1.1) with $\gcd(n, d) = 1$ implies that either $k = 4$ and $(n, d, b, y) = (75, 23, 6, 140)$, or $k = 5$ and $P(b) = k$. In fact, we shall derive the preceding result with $k \geq 10$ and $P(b) < k$ from Theorem 1 (see Corollary 3.11). We refer to [LaSh07] for results on (1.1) with $1 < \omega(d) \leq 4$.

2000 *Mathematics Subject Classification*: Primary 11D61.

Key words and phrases: diophantine equations, arithmetic progressions, Legendre symbol.

Let $\psi = 1$. We may assume that $\gamma_1 = 0$ and $\gamma_t = k-1$. It has been shown in [SaSh03b] that

$$\frac{6!}{5} = 12^2, \qquad \frac{10!}{7} = 720^2$$

are the only squares that are products of $k-1$ distinct integers out of k consecutive integers, confirming a conjecture of Erdős and Selfridge [ErSe75]. This corresponds to the case $b = 1$ and $d = 1$ in (1.1). In general, it has been proved in [SaSh03b] that (1.1) with $d = 1$ and $k \geq 4$ implies that $(b, k, n) = (2, 4, 24)$ under the necessary assumption that the left hand side of (1.1) is divisible by a prime $> k$. Further, it has been shown in [SaSh03a, Theorem 4] and [MuSh04a] that (1.1) with $d > 1$, $\gcd(n, d) = 1$, $\omega(d) = 1$ and $P(b) < k$ implies that $k \leq 8$. It is clear from the argument given at the end of this section that the assumption $\gcd(n, d) = 1$ can be relaxed to $d \nmid n$ in the results stated above for $\psi = 0$ and $\psi = 1$.

Let $\psi = 2$. As earlier for $\psi = 0$ and $\psi = 1$, we first turn to the case $d = 1$. Then it has been shown in [MuSh04b, Corollary 3] that a product of $k-2$ distinct terms out of k consecutive positive integers is a square only if it is given by

$$\frac{6!}{1 \cdot 5} = \frac{7!}{5 \cdot 7} = 12^2, \qquad \frac{10!}{1 \cdot 7} = \frac{11!}{7 \cdot 11} = 720^2,$$

and

$$\begin{cases} \dfrac{4!}{2 \cdot 3} = 2^2, \quad \dfrac{6!}{4 \cdot 5} = 6^2, \quad \dfrac{8!/2!}{5 \cdot 7} = 24^2, \quad \dfrac{10!/4!}{6 \cdot 7} = 60^2, \quad \dfrac{9!/2!}{5 \cdot 7} = 72^2, \\ \dfrac{10!/3!}{6 \cdot 7} = 120^2, \quad \dfrac{10!/2!}{7 \cdot 8} = 180^2, \quad \dfrac{10!}{7 \cdot 9} = 240^2, \quad \dfrac{10!}{4 \cdot 7} = 360^2, \\ \dfrac{21!/13!}{17 \cdot 19} = 5040^2, \quad \dfrac{14!/4!}{11 \cdot 13} = 5040^2, \quad \dfrac{14!/3!}{11 \cdot 13} = 10080^2. \end{cases}$$

The above result corresponds to (1.1) with $b = 1$. For the general case, we have

THEOREM 2. *Let $\psi = 2$, $d = 1$ and $k \geq 5$. Assume that the left hand side of (1.1) is divisible by a prime $> k$. Then (1.1) is valid if and only if $k = 5$ and $n \in \{45, 46, 47, 48, 96, 239, 240, 241, 242, 359, 360\}$, or $k = 6$ and $n \in \{45, 240\}$.*

We observe that $n + k - 1 \geq p^2_{\pi(k)+1} \geq (k+1)^2$, since the left hand side of (1.1) is divisible by a prime $> k$. Thus $n > k^2$ and the assertion for $k \geq 6$ follows immediately from [MuSh04b, Theorem 2]. Let $k = 5$. Then $n \geq 7^2 - 4 = 45$. Multiplying both sides of (1.1) by b^3 and putting $X = b(n + \gamma_2), Y = b^2 y$, we get the elliptic curve

$$Y^2 = X^3 + b(\gamma_1 + \gamma_3 - 2\gamma_2)X^2 + b^2(\gamma_1 - \gamma_2)(\gamma_3 - \gamma_2)X.$$

For each choice of triplet $(\gamma_1, \gamma_2, \gamma_3)$ with $0 \le \gamma_1 < \gamma_2 < \gamma_3 \le 4$ and for each $b \in \{1, 2, 3, 5, 6, 10, 15, 30\}$, we check for the integral points on the elliptic curve using MAGMA. Observing that $b \mid X$, $b^2 \mid Y$ and $X = b(n+\gamma_2) \ge 45b$, we find that all solutions of (1.1) are given by those listed in the assertion of Theorem 2. For instance, when $(\gamma_1, \gamma_2, \gamma_3) = (0, 2, 4)$ and $b = 3$, we have the curve $Y^2 = X^3 - 36X$ and the only integral point with $X \ge 45b$ is $X = 294, Y = 5040$. Then $n + 2 = 294/3 = 98$, giving $n = 96$, and we see that $96 \cdot 98 \cdot 100 = 3(8 \cdot 7 \cdot 10)^2$ gives a solution. All the exceptional cases come from

$$45 \cdot 48 \cdot 49 = 15(4 \cdot 3 \cdot 7)^2, \qquad 48 \cdot 49 \cdot 50 = 6(4 \cdot 5 \cdot 7)^2,$$
$$96 \cdot 98 \cdot 100 = 3(8 \cdot 7 \cdot 10)^2, \qquad 240 \cdot 242 \cdot 243 = 10(4 \cdot 27 \cdot 11)^2,$$
$$242 \cdot 243 \cdot 245 = 30(9 \cdot 7 \cdot 11)^2, \qquad 360 \cdot 361 \cdot 363 = 30(2 \cdot 3 \cdot 11 \cdot 19)^2.$$

We take $d > 1$ from now onwards in this paper. To solve (1.1) with $d \nmid n$, it suffices to assume that $\gcd(n, d) = 1$. Indeed, suppose $\gcd(n, d) > 1$. Let $p^\beta = \gcd(n, d)$, $n' = n/p^\beta$ and $d' = d/p^\beta$. Then $d' > 1$ since $d \nmid n$. Now, dividing both sides of (1.1) by $(p^\beta)^t$, we have

$$(n' + \gamma_1 d') \cdots (n' + \gamma_t d') = p^\varepsilon b' y'^2, \tag{1.2}$$

where $y' > 0$ is an integer, b' squarefree and $\varepsilon \in \{0, 1\}$. Since $p \mid d'$ and $\gcd(n', d') = 1$, we see that $p \nmid (n' + \gamma_1 d') \cdots (n' + \gamma_t d')$, giving $\varepsilon = 0$, and the assertion follows. Hence for the proof of Theorem 1 and other results on (1.1), we assume from now onwards that $\gcd(n, d) = 1$.

As in [ShTi90], the proofs depend on comparing an upper bound and a lower bound for $n + (k-1)d$. These estimates turn out to be considerable improvements of the ones obtained in [SaSh03a]. For example, in the case $\psi = 0$ and $\omega(d) = 1$, we get $k \le 31$ whereas in [SaSh03a], we obtain $k < 104$. This improvement is mainly due to sharp estimates from [LaSh07]. This is crucial for the proof of Theorem 1, as otherwise it would not have been feasible to cover all the values from $k = 15$ onwards in Theorem 1. To cover the values $15 \le k \le 31$, we further refine the method of Euler as developed in [HiLaShTi07]. Since we allow omitting one or two terms but we do not know which terms are being omitted, there would have been too many cases to consider if we had applied the method of [HiLaShTi07]; therefore, a refinement was necessary.

2. Notations and preliminaries. We assume (1.1) with $\gcd(n, d) = 1$ in this section. Then we have

$$n + \gamma_i d = a_{\gamma_i} x_{\gamma_i}^2 \quad \text{for } 1 \le i \le t \tag{2.1}$$

with a_{γ_i} squarefree such that $P(a_{\gamma_i}) \le \max(k-1, P(b))$. Also

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

with $P(A_{\gamma_i}) \le k$ 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 (2.1) and (2.2) that

$$(b_i,d) = (B_i,d) = (y_i,d) = (Y_i,d) = 1 \quad \text{for } 1 \le i \le t. \tag{2.3}$$

Let

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

For $b_{i_0} \in R$, let $\nu(b_{i_0}) = |\{j : 1 \le j \le t,\, b_j = b_{i_0}\}|$. 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 $i \in T_1$ and hence

$$n + (k-1)d \ge \max\{p^2_{|T_1|+\pi_d(k)}, |\{B_i : i \in T_1\}|k^2\}. \tag{2.4}$$

For $i_0 \in T_1$, we define $\nu(B_{i_0}) = |\{j \in T_1 : B_j = B_{i_0}\}|$.

Let

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

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

$$\theta = \begin{cases} 1 & \text{if } d = 2,4, \\ 0 & \text{otherwise.} \end{cases} \tag{2.7}$$

Let $d = p^\alpha$. Then we say (d_1,d_2) is a *partition* of d if $d = d_1d_2$ and $\gcd(d_1,d_2) = \eta$, and we take $(1,2)$ as the partition of $d = 2$. Further, $(2,2)$ is the only partition if $d = 4$. For $d \ne 2,4$, we see that $d \ne \eta^2$ and therefore $(\eta, d/\eta)$ and $(d/\eta, \eta)$ are the only distinct partitions of d. Let $b_i = b_j$, $i > j$. Then from (2.1) and (2.3), we have

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

such that $\gcd(d, y_i - y_j, y_i + y_j) = 2^{\delta'}$. 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 $d_1 \mid (y_i - y_j)$ and $d_2 \mid (y_i + y_j)$, and this partition is unique. Similarly, we have a unique partition of d corresponding to every pair (i,j) with $i > j$, $i,j \in T_1$ and $B_i = B_j$.

Let q be a prime $\le k$ and coprime to d. Then the number of i's for which b_i is divisible by q is at most $\sigma_q = \lceil k/q \rceil$. Let $\sigma'_q = |\{b_i : q \mid b_i\}|$. Then $\sigma'_q \le \sigma_q$. Let $r \ge 3$ be any positive integer. Define

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

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

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

We have

$$\xi_r \ge t - F(k,r) \ge t - F'(k,r) + \sum_{p|d,\, p>p_r} \sigma_p \tag{2.9}$$

and

$$\begin{aligned} t - |R| &\ge t - |\{b_i : P(b_i) > p_r\}| - |\{b_i : P(b_i) \le p_r\}| && (2.10)\\ &\ge t - F(k,r) - |\{b_i : P(b_i) \le p_r\}| && (2.11)\\ &\ge t - F'(k,r) + \sum_{p|d,\, p>p_r} \sigma_p - |\{b_i : P(b_i) \le p_r\}| && (2.12)\\ &\ge t - F'(k,r) + \sum_{p|d,\, p>p_r} \sigma_p - 2^r. && (2.13) \end{aligned}$$

We write $\mathcal{S} := \mathcal{S}(r)$ for the set of positive squarefree integers composed of primes $\le p_r$. Put $p = 2^\delta$ if d is even, and $p = P(d)$ if d is odd. Suppose $p = 2^\delta$. Then $b_i \equiv n \pmod{2^\delta}$. Considering elements of $\mathcal{S}(r)$ modulo 2^δ, we see by induction on r that

$$|\{b_i : P(b_i) \le p_r\}| \le 2^{r-\delta} =: g_{2^\delta}. \tag{2.14}$$

Let $p = P(d)$. Then all b_i's are either quadratic residues mod p or non-quadratic residues mod p. We consider two sets

$$\mathcal{S}_1(p,r) = \left\{ s \in \mathcal{S} : \left(\frac{s}{p}\right) = 1 \right\}, \qquad \mathcal{S}_2(p,r) = \left\{ s \in \mathcal{S} : \left(\frac{s}{p}\right) = -1 \right\} \tag{2.15}$$

and define

$$g_p(r) = \max(|\mathcal{S}_1(p,r)|, |\mathcal{S}_2(p,r)|). \tag{2.16}$$

Then

$$|\{b_i : P(b_i) \le p_r\}| \le g_p. \tag{2.17}$$

In view of (2.14) and (2.17), the inequality (2.12) is improved as

$$t - |R| \ge k - \psi - F'(k,r) + \sum_{p|d,\, p>p_r} \sigma_p - g_p. \tag{2.18}$$

Let $r = 3, 4$ and $2 < p \le 220$. Then we calculate

$$g_p(r) = \begin{cases} 2^{r-2} & \text{if } p \le p_r, \\ 2^{r-1} & \text{if } p > p_r, \end{cases} \tag{2.19}$$

except when $r = 3$ and $p \in \{71, 191\}$, where $g_p = 2^r$.

We close this section with the following lemmas which are independent of (1.1). The first lemma is an estimate on $\pi(x)$ due to Dusart [Dus99].

Lemma 2.1. *We have*

$$\pi(x) \le \frac{x}{\log x}\left(1 + \frac{1.2762}{\log x}\right) \quad \textit{for } x > 1.$$

The following lemma is contained in [LaSh04, Theorem 1].

Lemma 2.2. *Let* $k \ge 9$, $d > 1$, $\gcd(n,d) = 1$, $n > k$ *if* $d = 2$, *and* $(n,d,k) \notin V$, *where* V *is given by*

$$\begin{cases} n = 1,\ d = 3,\ k = 9, 10, 11, 12, 19, 22, 24, 31; \\ n = 2,\ d = 3,\ k = 12;\ n = 4,\ d = 3,\ k = 9, 10; \\ n = 2,\ d = 5,\ k = 9, 10; \\ n = 1,\ d = 7,\ k = 10. \end{cases} \tag{2.20}$$

Then

$$\begin{aligned} W(n(n+d)\cdots(n+(k-1)d)) &:= |\{i : 0 \le i < k, P(n+id) > k\}| \\ &\ge \pi(2k) - \pi_d(k). \end{aligned} \tag{2.21}$$

Let $d = 2$ *and* $n \le k$. *Then*

$$W(n(n+d)\cdots(n+(k-1)d)) \ge \pi(2k) - \pi_d(k) - 1. \tag{2.22}$$

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

Lemma 2.3. *Let* s_i *denote the* ith *squarefree positive integer. Then*

$$\prod_{i=1}^{l} s_i \ge (1.6)^l l! \quad \textit{for } l \ge 286. \tag{2.23}$$

3. Lemmas for the equation (1.1). All the lemmas in this section are under the assumption that (1.1) with $\gcd(n,d) = 1$ and $\omega(d) = 1$ is valid and we shall suppose it without further mention.

Lemma 3.1. *Let* ψ *be fixed. Suppose that* (1.1) *with* $P(b) \le k$ *has no solution at* $k = k_1$ *with* k_1 *prime. Then* (1.1) *with* $P(b) \le k$ *and* $k_1 \le k < k_2$ *has no solution, where* k_1, k_2 *are consecutive primes.*

Proof. Let k_1, k_2 be consecutive primes such that $k_1 \le k < k_2$. Suppose (n, d, b, y) is a solution of

$$(n + \gamma_1 d)\cdots(n + \gamma_t d) = by^2$$

with $P(b) \le k$. Then $P(b) \le k_1$. We observe that $\gamma_{k_1-\psi} < k_1$ and by (2.1),

$$(n + \gamma_1 d)\cdots(n + \gamma_{k_1-\psi} d) = b' y'^2$$

for some b' with $P(b') \le k_1$, giving a solution of (1.1) at $k = k_1$. This is a contradiction. ∎

In view of Lemma 3.1, there is no loss of generality in assuming that k is prime whenever $k \geq 23$ in the proof of Theorem 1. Therefore we suppose from now onward that k is prime if $k \geq 23$. The following lemma gives a lower bound for $|T_1|$ (see [LaSh07, Lemma 4.1]).

LEMMA 3.2. *Let $k \geq 4$. Then*

$$\begin{aligned}(3.1)\quad |T_1| > \\ & t - \frac{(k-1)\log(k-1) - \sum_{p \mid d,\, p<k} \max\bigl(0, \frac{(k-1-p)\log p}{p-1} - \log(k-2)\bigr)}{\log(n+(k-1)d)} \\ & - \pi_d(k) - 1.\end{aligned}$$

We apply Lemmas 2.2 and 3.2 to derive the following result.

COROLLARY 3.3. *Let $k \geq 9$. Then*

$$|T_1| > 0.1754k \quad \textit{for } k \geq 81, \tag{3.2}$$

and

$$n + \gamma_t d > \eta^2 k^2. \tag{3.3}$$

Proof. We observe that $\pi(2k) - \pi(k) > 2$ since $k \geq 9$. Therefore $P(\Delta) > k$ by Lemma 2.2. Now we see from (1.1) that

$$n + \gamma_t d > k^2. \tag{3.4}$$

From (3.1), $t \geq k-2$, $\pi_d(k) \leq \pi(k)$ and Lemma 2.1, we get

$$|T_1| > k - 3 - \frac{(k-1)\log k}{2\log k} - \frac{k}{\log k}\left(1 + \frac{1.2762}{\log k}\right).$$

Since the right hand side of the above inequality exceeds $0.1754k$ for $k \geq 81$, the assertion (3.2) follows.

Now we turn to the proof of (3.3). By (3.4), it suffices to consider $d = 2^\alpha$ with $\alpha > 1$. From Lemma 2.2 and (1.1), we have $n + (k-1)d > p^2_{\pi(2k)-2}$. Now we see from (3.1) that

$$\begin{aligned}(3.5)\quad & |T_1| + \pi_d(k) - \pi(2k) \\ & > k - 3 - \frac{(k-1)\log(k-1) - (k-3)\log 2 + \log(k-2)}{2\log p_{\pi(2k)-2}} - \pi(2k)\end{aligned}$$

and

$$\begin{aligned}& |T_1| + \pi_d(k) - \pi(2k) \\ & > k - 3 - \frac{(k-1)\log k - (k-3)\log 2 + \log k}{2\log k} - \frac{2k}{\log 2k}\left(1 + \frac{1.2762}{\log 2k}\right)\end{aligned}$$

by Lemma 2.1. When $k \geq 60$, the right hand side of the last inequality is positive. Therefore $|T_1| + \pi_d(k) > \pi(2k)$, implying $n + \gamma_t d > 4k^2$ for

$k \geq 60$. Thus we may assume $k < 60$. Now we can check that the right hand side of (3.5) is positive for $k \geq 33$. Therefore we may suppose that $k < 33$ and $n + (k-3)d \leq n + \gamma_t d \leq 4k^2$. Hence $d = 2^\alpha < 4k^2/(k-3)$. For n, d, k satisfying $k < 33$, $d < 4k^2/(k-3)$, $n + (k-3)d \leq 4k^2$ and $n+(k-1)d \geq p^2_{\pi(2k)-2}$, we check that there are at least three i with $0 \leq i < k$ such that $n + id$ is divisible by a prime $> k$ to the first power. This is not possible. ∎

The next lemma follows from (3.3) and [LaSh07, Lemma 3.5 and Corollary 3.7].

Lemma 3.4. *For any pair (i, j) with $b_i = b_j$, the partition $(d\eta^{-1}, \eta)$ of d is not possible. Further, $\nu(b_i) \leq 2^{1-\theta}$ and $\nu(B_i) \leq 2^{1-\theta}$.*

The following lemma follows from (3.3), Lemma 3.4 and [LaSh07, Lemma 3.9].

Lemma 3.5. *Assume that either d is odd or $8 \mid d$. Let $z_0 \in \{2, 3, 5\}$ be such that $z_0 = 5$ if $8 \mid d$. Further, let $d = \theta_1(k-1)^2$ and $n = \theta_2(k-1)^3$ with θ_1, $\theta_2 > 0$. Suppose that $t - |R| \geq z_0$. Then we have the partition $(\eta, d\eta^{-1})$ of d such that*

$$d\eta^{-1} < \frac{4(k-1)}{q_2} \tag{3.6}$$

and

$$\theta_2 < \frac{1}{2}\left\{\frac{1}{q_1q_2} - \theta_1 + \sqrt{\frac{1}{(q_1q_2)^2} + \frac{\theta_1}{q_1q_2}}\right\} \tag{3.7}$$

with $q_1 \geq Q_1$, $q_2 \geq Q_2$, where (Q_1, Q_2) is $(1, 1), (2, 2), (4, 4)$ according as $z_0 = 2, 3, 5$, respectively when d is odd, and $(Q_1, Q_2) = (2, 8)$ when $z_0 = 5$ and $8 \mid d$.

Lemma 3.6. *Let $z_1 > 1$ be a real number, and $h_0 > i_0 \geq 0$ 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*

$$g_1 > \frac{k \log\left(\frac{z_1 \mathfrak{n}_0}{2.71851} \prod_{p \leq \mathfrak{m}} p^{\frac{2}{p^2-1}}\right) + \left(k + \frac{1}{2}\right) \log\left(1 - \frac{g_1}{k}\right)}{\log(k - g_1) - 1 + \log z_1} - \frac{(1.5\pi(\mathfrak{m}) - .5\ell - 1)\log k + \log\left(\mathfrak{n}_1^{-1}\mathfrak{n}_2 \prod_{p \leq \mathfrak{m}} p^{.5 + \frac{2}{p^2-1}}\right)}{\log(k - g_1) - 1 + \log z_1}, \tag{3.8}$$

where $\ell = |\{p \le \mathfrak{m} : p \mid d\}|$ *and*

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

For a proof, see [LaSh07, Lemma 5.4]. The assumption $\omega(d) = 1$ is not necessary for Lemmas 3.1, 3.2, 3.6 and Corollary 3.3.

Lemma 3.7. *We have*

$$t - |R| \ge \begin{cases} 5 & \textit{for } k \ge 81,\\ 5-\psi & \textit{for } k \ge 55,\\ 4-\psi & \textit{for } k\ge 28,\ k\ne 31,\\ 3-\psi & \textit{for } k = 31.\end{cases} \tag{3.9}$$

Proof. Suppose $t - |R| < 5$ and $k \ge 292$. Then $|R| \ge 286$ since $t \ge k-2$ and $\prod_{b_i\in R} b_i \ge (1.6)^{|R|}(|R|)!$ by (2.23). We observe that (3.8) holds for $k \ge 292$ with $i_0 = 0$, $h_0 = 286$, $z_1 = 1.6$, $g_1 = 6$, $\mathfrak{m} = 17$, $\ell = 0$, $\mathfrak{n}_0 = 1$, $\mathfrak{n}_1 = 1$ and $\mathfrak{n}_2 = 2^{1/6}$. We check that the right hand side of (3.8) is an increasing function of k and it exceeds g_1 at $k = 292$, which is a contradiction. Therefore $t - |R| \ge 5$ for $k \ge 292$. Thus we may assume that $k < 292$. By taking $r = 3$ for $k < 50$, $r = 4$ for $50 \le k \le 181$, and $r = 5$ for $181 < k < 292$ in (2.11) and (2.13), we get $t-|R| \ge k-\psi-F'(k,r)-2^r \ge 7-\psi, 5-\psi, 4-\psi$ for $k \ge 81, 55, 28$, respectively except at $k = 29, 31, 43, 47$, where $t-|R| \ge k-\psi-F(k,r)-2^r \ge k-\psi-F'(k,r)-2^r = 3-\psi$. We may suppose that $k = 29, 43, 47$, $t-|R| = 3-\psi$ and $F(k,r) = F'(k,r)$. Further, we may assume that for each prime $7 \le p \le k$, there are exactly σ_p i's for which $p \mid b_i$, and for any i, $pq \nmid b_i$ whenever $7 \le q \le k$ and $q \ne p$. Now we get a contradiction by considering the i's for which b_i's are divisible by primes $7, 13; 7, 41; 23, 11$ when $k = 29, 43, 47$, respectively.

For instance, let $k = 29$. Then $7 \mid b_i$ for $i \in \{0, 7, 14, 21, 28\}$. Hence $13 \mid b_i$ for $i \in \{h + 13j : 0 \le j \le 2\}$ with $h = 0, 1, 2$. This is not possible since otherwise $7\cdot 13 \mid b_i$ for some $i \in \{0, 14, 28\}$, a contradiction. ∎

Lemma 3.8. *Let* $9 \le k \le 23$ *and* d *odd. Suppose that* $t - |R| \ge 3$ *if* $k = 23$, *and* $t - |R| \ge 2$ *if* $k < 23$. *Then* (1.1) *does not hold.*

Proof. Suppose (1.1) holds. Let $Q = 2$ if $k = 23$, and $Q = 1$ if $k < 23$. We now apply Lemma 3.5 with $z_0 = 3$ for $k = 23$, and $z_0 = 2$ for $k < 23$, to get $d < \frac{4}{Q}(k-1)$, $\theta_1 < \frac{4}{Q(k-1)}$ and

$$\theta_1 + \theta_2 < \frac{1}{2}\left\{\frac{1}{Q^2} + \frac{4}{Q(k-1)} + \sqrt{\frac{1}{Q^4} + \frac{4}{Q^3(k-1)}}\right\} =: \Omega(k-1),$$

giving $n + (k-1)d = (\theta_1+\theta_2)(k-1)^3 < (k-1)^3\Omega(k-1)$. Further, from (2.4) and (2.21), we get $n + (k-1)d \ge n + \gamma_t d \ge p^2_{\pi(2k)-2}$. Therefore

$p^\alpha = d < \frac{4}{Q}(k-1)$ and $p^2_{\pi(2k)-2} \le n + (k-1)d < (k-1)^3\Omega(k-1)$; the latter inequality follows from the definitions of θ_1, θ_2 and $\Omega(k-1)$. For these possibilities of n, d and k, we check that there are at least three i's with $0 \le i < k$ such that $n + id$ is divisible by a prime $> k$ to an odd power. This contradicts (1.1). ∎

LEMMA 3.9. *Equation* (1.1) *with* $k \ge 9$ *implies that* $t - |R| \le 1$.

Proof. Assume that $k \ge 9$ and $t - |R| \ge 2$. Let $d = 2$ or 4. Then $|R| \le t - 2$, contradicting $|R| = t$ by Lemma 3.4. Thus $d \ne 2, 4$. By Lemma 3.4, we have $\nu(b_{i_0}) \le 2$ and $\nu(B_{i_0}) \le 2$.

Let $k \ge 81$. Then $t - |R| \ge 5$ by Lemma 3.7. Now from Lemma 3.5 with $z_0 = 5$ we derive that $d < k - 1$, giving $\theta_1 < \frac{1}{k-1}$ and hence

$$\begin{aligned} n + (k-1)d &= (\theta_1 + \theta_2)(k-1)^3 \\ &< \frac{(k-1)^3}{2}\left\{\frac{1}{16} + \frac{1}{k-1} + \sqrt{\frac{1}{(16)^2} + \frac{1}{16(k-1)}}\right\}. \end{aligned}$$

On the other hand, from (2.4), (3.2) and $\nu(B_i) \le 2$ for $i \in T_1$ we get

$$n + (k-1)d \ge \frac{|T_1|}{2}\,k^2 \ge \frac{0.1754k}{2}\,k^2 \ge 0.1754\,\frac{k^3}{2}.$$

Comparing the upper and lower bounds of $n + (k-1)d$, we obtain

$$0.1754 < \left\{\frac{1}{16} + \frac{1}{k-1} + \sqrt{\frac{1}{(16)^2} + \frac{1}{16(k-1)}}\right\} \le 0.144$$

since $k \ge 81$. This is a contradiction.

Thus $k < 81$. Let d be even. Then $8 \mid d$ and we see from $\nu(a_i) \le 2$ and (2.14) that $\xi_r \le 2g_{2^\delta} \le 2^{r-2}$. Let $r = 3$. From (2.9), we get $k - 2 - F'(k,r) \le \xi_r \le 2^{r-2}$. We find $k - 2 - F'(k,r) > 2^{r-2}$ by computation. This is a contradiction.

Thus d is odd. Since $\psi \le 2$, we deduce from Lemmas 3.7 and 3.5 with $z_0 = 3, 2$ that $d < 2(k-1)$ if $k \ge 55$, and $d < 4(k-1)$ if $k < 55$. Since $g_p(r) \le 2^{r-1}$ for $r = 4$ and $p < 220$ by (2.19), we infer from (2.18) with $r = 4$ that $t - |R| \ge k - 2 - F'(k,r) - 2^{r-1}$, which is ≥ 5 for $k \ge 29$, and ≥ 3 for $k = 23$.

Let $k \ge 29$. Then Lemma 3.5 with $z_0 = 5$ shows that $d < k - 1$. By taking $r = 3$ for $k < 53$, and $r = 4$ for $53 \le k < 81$, we derive from (2.17), (2.19), $\nu(a_i) \le 2$ and (2.9) that $k - 2 - F'(k,r) \le \xi_r \le 2g_p \le 2^r$. On the other hand, we check by computation that $k - 2 - F'(k,r) > 2^r$. This is a contradiction.

Thus $k \le 23$. Then $t - |R| \ge 3$ for $k = 23$, and $t - |R| \ge 2$ for $k < 23$. By Lemma 3.8, this is not possible. ∎

COROLLARY 3.10. *Let* $k \geq 9$. *Equation* (1.1) *with* $\gcd(n, d) = 1$ *and* $\omega(d) = 1$ *implies that either* $k \leq 23$ *or* $k = 31$. *Also* $P(d) > k$.

Proof. By Lemmas 3.7 and 3.9, either $k \leq 23$ or $k = 31$. Suppose that $P(d) \leq k$. Since $g_{P(d)}(r) \leq 2^{r-1}$ for $r = 3$ by (2.19), we find from (2.18) with $r = 3$ that $t - |R| \geq k - 2 - F'(k, r) - 2^{r-1} \geq 2$ except at $k = 9$, where $t - |R| = 1$. This contradicts Lemma 3.9 for $k > 9$. Let $k = 9$. By taking $r = 4$, we deduce from $g_{P(d)}(r) \leq 2^{r-2}$ by (2.19) and (2.18) that $t - |R| \geq k - 2 - F'(k, 4) - 2^{4-2} \geq 2$. This contradicts Lemma 3.9. ∎

As a direct consequence, we give a simpler proof of [SaSh03a, Theorem 1(ii)].

COROLLARY 3.11. *Let* $\psi = 0$. *Equation* (1.1) *with* $\gcd(n, d) = 1, \omega(d) = 1$ *and* $P(b) < k$ *implies that* $k \leq 9$.

As mentioned in Section 1, the assumption $\gcd(n, d) = 1$ can be relaxed to $d \nmid n$.

Proof. Let $k \geq 10$. By Corollary 3.10, either $k \leq 23$ or $k = 31$. Let $k = 10$. Then (2.13) with $r = 2$ shows that $t - |R| \geq k - F'(k, r) - 2^r = 2$, contradicting Lemma 3.9. Thus (1.1) does not hold at $k = 10$. By induction, we may assume $k \in \{12, 14, 18, 20\}$ and that there is at most one i for which $p \mid a_i$ with $p = k - 1$. We take $r = 2$ for $k = 12, 14$, and $r = 3$ for $k = 18, 20$. Now from $|\{b_i : P(b_i) > p_r\}| \leq F'(k, r) - 1$ and (2.10) we get $t - |R| \geq k - F'(k, r) + 1 - 2^r \geq 2$. This contradicts Lemma 3.9. ∎

4. Proof of Theorem 1. Suppose that the assumptions of Theorem 1 are satisfied and assume (1.1) with $\omega(d) = 1$. By Corollary 3.10, we have $P(d) > k$, and we restrict to $k \leq 23$ and $k = 31$. Also $t - |R| \leq 1$ by Lemma 3.9. Further, it suffices to prove the assertion for $k \in \{15, 17, 19, 23, 31\}$, since the cases $k = 16, 18$ and $k = 20, 21, 22$ follow from those of $k = 15, 17$ and 19, respectively.

We shall arrive at a contradiction by showing $t - |R| \geq 2$. For a prime $p \leq k$, we observe that $p \nmid d$, and let i_p be such that $0 \leq i_p < p$ and $p \mid n + i_p d$. For any subset $\mathcal{I} \subseteq [0, k) \cap \mathbb{Z}$ and primes p_1 and p_2, we define

$$\mathcal{I}_1 = \left\{ i \in \mathcal{I} : \left(\frac{i - i_{p_1}}{p_1}\right) = \left(\frac{i - i_{p_2}}{p_2}\right) \right\},$$
$$\mathcal{I}_2 = \left\{ i \in \mathcal{I} : \left(\frac{i - i_{p_1}}{p_1}\right) \neq \left(\frac{i - i_{p_2}}{p_2}\right) \right\}.$$

Then from $\left(\frac{a_i}{p}\right) = \left(\frac{i - i_p}{p}\right)\left(\frac{d}{p}\right)$, we see that either

$$\left(\frac{a_i}{p_1}\right) \neq \left(\frac{a_i}{p_2}\right) \text{ for all } i \in \mathcal{I}_1 \quad \text{and} \quad \left(\frac{a_i}{p_1}\right) = \left(\frac{a_i}{p_2}\right) \text{ for all } i \in \mathcal{I}_2, \tag{4.1}$$

or

$$\left(\frac{a_i}{p_1}\right) \neq \left(\frac{a_i}{p_2}\right) \text{ for all } i \in \mathcal{I}_2 \quad \text{and} \quad \left(\frac{a_i}{p_1}\right) = \left(\frac{a_i}{p_2}\right) \text{ for all } i \in \mathcal{I}_1. \tag{4.2}$$

We define $(\mathcal{M}, \mathcal{B}) = (\mathcal{I}_1, \mathcal{I}_2)$ in the case (4.1), and $(\mathcal{M}, \mathcal{B}) = (\mathcal{I}_2, \mathcal{I}_1)$ in the case (4.2). We write $(\mathcal{I}_1, \mathcal{I}_2, \mathcal{M}, \mathcal{B}) = (\mathcal{I}_1^k, \mathcal{I}_2^k, \mathcal{M}^k, \mathcal{B}^k)$ when $\mathcal{I} = [0, k) \cap \mathbb{Z}$. Then for any $\mathcal{I} \subseteq [0, k) \cap \mathbb{Z}$, we have

$$\mathcal{I}_1 \subseteq \mathcal{I}_1^k, \quad \mathcal{I}_2 \subseteq \mathcal{I}_2^k, \quad \mathcal{M} \subseteq \mathcal{M}^k, \quad \mathcal{B} \subseteq \mathcal{B}^k$$

and

$$|\mathcal{M}| \geq |\mathcal{M}^k| - (k - |\mathcal{I}|), \quad |\mathcal{B}| \geq |\mathcal{B}^k| - (k - |\mathcal{I}|). \tag{4.3}$$

By taking $m = n + \gamma_t d$ and $\gamma_i' = \gamma_t - \gamma_{t-i+1}$, we rewrite (1.1) as

$$(m - \gamma_1' d) \cdots (m - \gamma_t' d) = by^2. \tag{4.4}$$

The equation (4.4) is called the *mirror image* of (1.1). The corresponding t-tuple $(a_{\gamma_1'}, \ldots, a_{\gamma_t'})$ is called the *mirror image* of $(a_{\gamma_1}, \ldots, a_{\gamma_t})$.

4.1. *The case $k = 15$.* Then $\sigma_7' = 3$ implies that $7 \mid a_{7j}$ for $j = 0, 1, 2$, whereas $\sigma_7' \leq 2$ if $7 \nmid a_0 a_7 a_{14}$. Similarly $\sigma_{13}' = 2$ implies $13 \mid a_0, 13 \mid a_{13}$ or $13 \mid a_1, 13 \mid a_{14}$, whereas $\sigma_{13}' \leq 1$ otherwise. Thus $|\{a_i : 7 \mid a_i \text{ or } 13 \mid a_i\}| \leq 4$. It suffices to have

$$|\{a_i : p \mid a_i \text{ for } 5 \leq p \leq 13\}| \leq 7, \tag{4.5}$$

since then $t - |R| \geq k - 2 - |\{a_i : p \mid a_i \text{ for } 5 \leq p \leq 13\}| - 4 \geq 2$ by (2.10) with $r = 2$, a contradiction.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \ldots, \gamma_t\}$. We observe that $P(a_i) \leq 7$ for $i \in \mathcal{M} \cup \mathcal{B}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for each prime $q < k$ other than $5, 11, 13$, we observe that $5 \mid a_i$ whenever $i \in \mathcal{M}$. Since $\sigma_5 \leq 3$ and $|\mathcal{I}| = k - 2$, we deduce from (4.3) that $|\mathcal{M}^k| \leq 5$ and $5 \mid a_i$ for at least $|\mathcal{M}^k| - 2$ i's with $i \in \mathcal{M}^k$. Further, $5 \nmid a_i$ for $i \in \mathcal{B}$.

By taking the mirror image (4.4) of (1.1), we may suppose that $0 \leq i_{13} \leq 7$. For each possibility $0 \leq i_{11} < 11$ and $0 \leq i_{13} \leq 7$, we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$ and restrict to those pairs (i_{11}, i_{13}) with $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 5$. We see from $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 6$ that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality, and hence $\mathcal{B}^k$ is the other. Now we restrict to those pairs (i_{11}, i_{13}) for which there are at most two elements $i \in \mathcal{M}^k$ such that $5 \nmid a_i$. There are 31 such pairs. By counting the multiples of 11 and 13 and also the maximum multiples of 5 in $\mathcal{M}^k$ and the maximum number of multiples of 7 in $\mathcal{B}^k$, we again restrict to those pairs (i_{11}, i_{13}) which do not satisfy (4.5). With this procedure, all pairs (i_{11}, i_{13}) are excluded other than

$$(0, 6),\ (1, 3),\ (2, 4),\ (3, 5),\ (4, 6),\ (5, 3). \tag{4.6}$$

We first explain the procedure by showing how $(i_{11}, i_{13}) = (0, 0)$ is excluded. Now $\mathcal{M}^k = \{5, 10\}$ and $\mathcal{B}^k = \{1, 2, 3, 4, 6, 7, 8, 9, 12, 14\}$. Then there are three multiples of 11 and 13, at most two multiples of 5 in $\mathcal{M}^k$ and at most two multiples of 7 in $\mathcal{B}^k$, implying (4.5). Thus $(i_{11}, i_{13}) = (0, 0)$ is excluded.

Let $(i_{11}, i_{13}) = (5, 3)$. Then $\mathcal{M}^k = \{1, 6, 11\}$ and $\mathcal{B}^k = \{0, 2, 4, 7, 8, 9, 10, 12, 13, 14\}$, giving $i_5 = 1$ and $5 \mid a_1 a_6 a_{11}$. We may assume that $7 \mid a_i$ for $i \in \{0, 7, 14\}$, as otherwise (4.5) holds. By taking $p_1 = 5$, $p_2 = 11$ and $\mathcal{I} = \mathcal{B}^k$, we get $\mathcal{I}_1 = \{4, 10, 13\}$ and $\mathcal{I}_2 = \{0, 2, 7, 8, 9, 12, 14\}$. Since $\left(\frac{2}{5}\right) = \left(\frac{2}{11}\right)$, $\left(\frac{7}{5}\right) = \left(\frac{7}{11}\right)$ and $\left(\frac{3}{5}\right) \neq \left(\frac{3}{11}\right)$, we observe that $3 \mid a_i$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$ and $3 \nmid a_i$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$. Thus $a_i \in \{3, 6\}$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$, and $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$. Now from $\left(\frac{a_i}{7}\right) = \left(\frac{i-0}{7}\right)\left(\frac{d}{7}\right)$ and $\left(\frac{3}{7}\right) = \left(\frac{6}{7}\right)$, we see that at least one of $4, 10, 13$ is not in $\mathcal{B}$, implying $i \notin \mathcal{B}$ for at most one $i \in \mathcal{I}_2$. Therefore there are distinct pairs (i_1, i_2) and (j_1, j_2) with $i_1, i_2, j_1, j_2 \in \mathcal{I}_2 \cap \mathcal{B}$ such that $a_{i_1} = a_{i_2}$, $i_1 > i_2$, and $a_{j_1} = a_{j_2}$, $j_1 > j_2$, giving $t - |R| \geq 2$. This is a contradiction. Similarly, all other pairs (i_{11}, i_{13}) in (4.6) are excluded.

4.2. *The case $k = 17$.* We may assume that $\sigma'_{17} = 1$ and $17 \nmid a_0 a_1 a_{15} a_{16}$, as otherwise the assertion follows from the case $k = 15$. If $|\{a_i : P(a_i) = 5\}| = 4$, we see from $\{a_i : P(a_i) = 5\} \subseteq \{5, 10, 15, 30\}$ that $a_{i_5} a_{i_5+5} a_{i_5+10} a_{i_5+15} = 150^2$, implying $(n + i_5 d)(n + (i_5 + 5)d)(n + (i_5 + 10)d)(n + (i_5 + 15)d)$ is a square, contradicting Euler's result for $k = 4$. Thus we have $|\{a_i : P(a_i) = 5\}| \leq 3$. It suffices to have

$$|\{a_i : p \mid a_i \text{ for } 5 \leq p \leq 17\}| \leq 9, \tag{4.7}$$

since then $t - |R| \geq k - 2 - |\{a_i : p \mid a_i \text{ for } 5 \leq p \leq 17\}| - 4 \geq 2$ by (2.10) with $r = 2$, a contradiction. Further, for each prime $7 \leq p \leq 13$, we may also assume that $\sigma'_p \geq 1$, as otherwise $t - |R| \geq k - 2 - \sum_{7 \leq p \leq 17} \sigma'_p - 3 - 4 \geq 2$ by (2.10) with $r = 2$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \ldots, \gamma_t\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ and $\left(\frac{17}{11}\right) \neq \left(\frac{17}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q < k$, $q \neq 5, 17, 11, 13$, we observe that for $i \in \mathcal{M}$, exactly one of $5 \mid a_i$ or $17 \mid a_i$ holds. Thus $5 \cdot 17 \nmid a_i$ whenever $i \in \mathcal{M}$. For $i \in \mathcal{B}$, either $5 \nmid a_i$ and $17 \nmid a_i$, or $5 \mid a_i$ and $17 \mid a_i$. Thus for $i \in \mathcal{B}$, we have $P(a_i) \leq 7$ except possibly for one i for which $5 \cdot 17 \mid a_i$. Since $\sigma_5 \leq 4$ and $\sigma'_{17} \leq 1$, we deduce from (4.3) that $|\mathcal{M}^k| \leq 7$ and $5 \mid a_i$ for at least $|\mathcal{M}^k| - 3$ elements i with $i \in \mathcal{M}^k$.

By taking the mirror image (4.4) of (1.1), we may suppose that $0 \leq i_{13} \leq 8$. Also we have $0 \leq i_{11} < 11$. Further, $i_{11} \leq 5$ if $i_{13} \geq 4$, and $i_{13} \leq 3$ if $i_{11} \geq 6$, as otherwise (4.7) follows, a contradiction. For each of these possible pairs (i_{11}, i_{13}), we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$. We find that there are 20 pairs (i_{11}, i_{13}) for which $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) = 7$. For each of these pairs, we find that $5 \mid a_i$ for at most $|\mathcal{I}_1^k| - 4$ i's with $i \in \mathcal{I}_1^k$, and $5 \mid a_i$ for at most $|\mathcal{I}_2^k| - 4$ i's with $i \in \mathcal{I}_2^k$. Hence these pairs are all excluded. For the remaining pairs (i_{11}, i_{13}), we infer from $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 8$ that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality, and hence $\mathcal{B}^k$ is the other. Now we restrict to those pairs (i_{11}, i_{13}) for which $5 \mid a_i$ for at least $|\mathcal{M}^k| - 3$ elements $i \in \mathcal{M}^k$. We may assume that $5 \mid a_i$ for at least two elements $i \in \mathcal{M}^k$, as otherwise (4.7) follows, a contradiction. Now we check for the inequality (4.7) by counting the multiples of $11, 13$ given by i_{11}, i_{13}, multiples of $5, 17$ in $\mathcal{M}^k \cup \mathcal{B}^k$, and maximum multiples of 7 in $\mathcal{B}^k$. We find that all the pairs other than $(i_{11}, i_{13}) \in \{(1,3), (2,4), (3,5), (4,0), (4.6)\}$ satisfy (4.7), and hence they are excluded. For instance, let $(i_{11}, i_{13}) = (0, 2)$. Then we get $\mathcal{M}^k = \{4, 6, 9\}$ and $\mathcal{B}^k = \{1, 3, 5, 7, 8, 10, 12, 13, 14, 16\}$. Now $5 \mid a_i$ for $i \in \{4, 9\}$, either $17 \mid a_6$ or $6 \notin \mathcal{M}$ and $5 \cdot 17 \mid a_{14}$. Further, there are at most two elements $i \in \mathcal{B}^k$ for which $7 \mid a_i$, giving (4.7). Thus we now restrict to $(i_{11}, i_{13}) \in \{(1,3), (2,4), (3,5), (4,0), (4,6)\}$.

Let $(i_{11}, i_{13}) = (1, 3)$. We have $\mathcal{M}^k = \{0, 5, 7, 10\}$ and $\mathcal{B}^k = \{2, 4, 6, 8, 9, 11, 13, 14, 15\}$, giving $i_5 = 0$ and $5 \mid a_0 a_5 a_{10}$. We may assume that $17 \mid a_7$ since $17 \nmid a_{15}$, giving $i_{17} = 7$. Hence $P(a_i) \le 7$ for $i \in \mathcal{B}$. Thus there are two elements $i \in \mathcal{B}^k$ which are not in $\mathcal{B}$, and $P(a_i) \le 7$ for the remaining seven elements $i \in \mathcal{B}^k$. Further, $7 \mid a_{i_7}$ and $7 \mid a_{i_7+7}$ for some $i_7 \in \{2, 4, 6, 8\}$ and $i_7, i_7 + 7 \in \mathcal{B}$, as otherwise $t - |R| \ge 2$. For each choice of $i_7 \in \{2, 4, 6, 8\}$ and $i_{17} = 7$, we now take $p_1 = 7$, $p_2 = 17$, $\mathcal{I} = \mathcal{B}^k$ and compute $\mathcal{I}_1$ and $\mathcal{I}_2$. Since $\left(\frac{2}{7}\right) = \left(\frac{2}{17}\right)$, $\left(\frac{3}{7}\right) = \left(\frac{3}{17}\right)$, we observe that either $\mathcal{I}_1 \cap \mathcal{B} = \emptyset$ and $a_i \in \{1, 2, 3, 6\}$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$, or $\mathcal{I}_2 \cap \mathcal{B} = \emptyset$ and $a_i \in \{1, 2, 3, 6\}$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$. From $\psi = 2$, we obtain either $|\mathcal{I}_1| \le 2$ or $|\mathcal{I}_2| \le 2$, giving $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \le 2$. We find that $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \ge 3$ except when $i_7 = 4$, where $\mathcal{I}_1 = \{2, 6, 8, 14, 15\}$ and $\mathcal{I}_2 = \{9, 13\}$. Thus $\mathcal{I}_2 \cap \mathcal{B} = \emptyset$, $\mathcal{I}_1 \subseteq \mathcal{B}$ and $a_i \in \{1, 2, 3, 6\}$ for $i \in \mathcal{I}_1$. From $\left(\frac{a_i}{7}\right) = \left(\frac{i-4}{7}\right)\left(\frac{d}{7}\right)$, $\left(\frac{i-4}{7}\right) = 1$ for $i \in \{6, 8, 15\}$, $\left(\frac{i-4}{7}\right) = -1$ for $i \in \{2, 14\}$, and $\left(\frac{a_i}{7}\right) = 1$ for $a_i \in \{1, 2\}$, $\left(\frac{a_i}{7}\right) = -1$ for $a_i \in \{3, 6\}$, we obtain $a_i \in \{1, 2\}$ for $i \in \{6, 8, 15\}$, and $a_i \in \{3, 6\}$ for $i \in \{2, 14\}$. Further, from $5 \mid n$, we get $\left(\frac{a_i}{5}\right) = \left(\frac{i}{5}\right)\left(\frac{d}{5}\right) = \left(\frac{d}{5}\right)$ for $i \in \{6, 14\}$, and $\left(\frac{a_i}{5}\right) = \left(\frac{i-0}{5}\right)\left(\frac{d}{5}\right) = -\left(\frac{d}{5}\right)$ for $i \in \{2, 8\}$. This together with $\left(\frac{a_i}{5}\right) = 1$ for $a_i \in \{1, 6\}$ and $\left(\frac{a_i}{5}\right) = -1$ for $a_i \in \{2, 3\}$ implies that either $a_6 = a_{15} = 1$, $a_8 = 2$, $a_2 = 3$, $a_{14} = 6$, or $a_6 = 2$, $a_8 = a_{15} = 1$, $a_2 = 6$, $a_{14} = 3$. The former possibility is excluded by Runge's method as in [MuSh03], and the latter possibility is excluded since $-1 = \left(\frac{a_6 a_{15}}{3}\right) = \left(\frac{(6-2)(15-2)}{3}\right) = 1$. The other cases $(i_{11}, i_{13}) \in \{(2,4), (3,5), (4,0), (4,6)\}$ are excluded similarly. In fact, in the cases $(i_{11}, i_{13}) = (2,4), (3,5)$, we obtain $(i_7, i_{17}) = (5, 8)$, $|\mathcal{I}_1| = 6$, $|\mathcal{I}_2| = 2$ and $(i_7, i_{17}) = (6, 9)$, $|\mathcal{I}_1| = 6$, $|\mathcal{I}_2| = 2$, respectively, implying $t - |R| \ge 2$ and hence these cases are excluded. In the case $(i_{11}, i_{13}) = (4, 6)$, we obtain $i_7 = 0$, $i_{17} = 10$, $a_i \in \{1, 2\}$ for $i \in \{1, 2, 9, 11\}$ and $a_5 \in \{3, 6\}$, giving $t - |R| \ge 2$. In the case $(i_{11}, i_{13}) = (4, 0)$, we obtain either $a_1 = a_{10} = 1$, $a_8 = 2$, $a_2 = 6$, $a_{14} = 3$, which is excluded by Runge's method as in [MuSh03], or $a_1 = a_8 = 1$, $a_{10} = 2$, $a_2 = 3$, $a_{14} = 6$, which is excluded modulo 3.

4.3. *The case $k = 19$.* We may assume that $\sigma'_{19} = 1$ and $19 \nmid a_0a_1a_{17}a_{18}$, as otherwise the assertion follows from the case $k = 17$. As in the case $k = 17$, we also have $|\{a_i : P(a_i) = 5\}| \le 3$ by Euler's result for $k = 4$. It suffices to have

$$|\{a_i : p \mid a_i \text{ for } 5 \le p \le 19\}| \le 11, \tag{4.8}$$

since then $t - |R| \ge k - 2 - |\{a_i : p \mid a_i \text{ for } 5 \le p \le 19\}| - 4 \ge 2$ by (2.10) with $r = 2$, a contradiction. Further, for each prime $7 \le p \le 13$, we may also assume that $\sigma'_p \ge 1$, as otherwise $t - |R| \ge k - 2 - \sum_{7 \le p \le 17} \sigma'_p - 3 - 4 \ge 2$ by (2.10) with $r = 2$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \ldots, \gamma_t\}$. Then as in the case $k = 17$, we observe that for $i \in \mathcal{M}$, exactly one of $5 \mid a_i$ or $17 \mid a_i$ holds but $5 \cdot 17 \nmid a_i$. For $i \in \mathcal{B}$, either $5 \nmid a_i$ and $17 \nmid a_i$, or $5 \mid a_i$ and $17 \mid a_i$. Since $\sigma_5 \le 4$ and $\sigma_{17} \le 2$, we deduce from (4.3) that $|\mathcal{M}^k| \le 8$ and $5 \mid a_i$ for at least $|\mathcal{M}^k| - 4$ elements $i \in \mathcal{M}^k$.

By taking the mirror image (4.4) of (1.1), we may suppose that $0 \le i_{13} \le 9$. Also we have $0 \le i_{11} < 11$. Further, $i_{11} \le 7$ if $i_{13} \ge 6$, and $i_{13} \le 5$ if $i_{11} \ge 8$, as otherwise (4.8) follows, a contradiction. For each of these possible pairs (i_{11}, i_{13}), we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$. We find that there are 27 pairs (i_{11}, i_{13}) for which $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) = 8$. For each of these pairs, we find that $5 \mid a_i$ or $17 \mid a_i$ for at most $|\mathcal{I}_1^k| - 3$ elements $i \in \mathcal{I}_1^k$, and $5 \mid a_i$ or $17 \mid a_i$ for at most $|\mathcal{I}_2^k| - 3$ elements $i \in \mathcal{I}_2^k$. Hence these pairs are all excluded. For the remaining pairs (i_{11}, i_{13}), we infer from $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \ge 9$ that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality, and hence $\mathcal{B}^k$ is the other.

Now we restrict to those pairs (i_{11}, i_{13}) for which $5 \mid a_i$ or $17 \mid a_i$ for at least $|\mathcal{M}^k| - 2$ elements $i \in \mathcal{M}^k$. We may assume that $5 \mid a_i$ for at least two elements $i \in \mathcal{M}^k$, as otherwise (4.7) follows, a contradiction. Now we check for the inequality (4.8) by counting the multiples of $11, 13$ given by i_{11}, i_{13}, multiples of $5, 17$ in $\mathcal{M}^k \cup \mathcal{B}^k$ and maximum multiples of $7, 19$ in $\mathcal{B}^k$. We find that all the pairs other than $(i_{11}, i_{13}) \in \{(1,3), (2,4), (3,5), (4,0), (5,1), (6,2)\}$ satisfy (4.8), and hence they are excluded. Thus we now restrict to $(i_{11}, i_{13}) \in \{(1,3), (2,4), (3,5), (4,0), (5,1), (6,2)\}$.

Let $(i_{11}, i_{13}) = (5,1)$. We have $\mathcal{M}^k = \{7, 10, 12, 17\}$ and $\mathcal{B}^k = \{0, 2, 3, 4, 6, 8, 9, 11, 13, 15, 18\}$, giving $i_5 = 2$ and $5 \mid a_7a_{12}a_{17}$. Further, $7 \mid a_i$ for $i \in \{4, 11, 18\} \subseteq \mathcal{B}$, as otherwise (4.8) is satisfied. Hence $i_7 = 4$. Now either $17 \mid a_{10}$, or $10 \notin \mathcal{M}$ and $5 \cdot 17 \mid a_2$, giving $i_{17} \in \{2, 10\}$. For these choices of i_7, i_{17}, we take $p_1 = 7$, $p_2 = 17$ and $\mathcal{I} = \mathcal{B}^k$ to compute $\mathcal{I}_1$ and $\mathcal{I}_2$. We observe that either $19 \mid a_i$ or $P(a_i) \le 3$ for $i \in (\mathcal{I}_1 \cup \mathcal{I}_2) \cap \mathcal{B}$. Since $\left(\frac{2}{7}\right) = \left(\frac{2}{17}\right)$ and $\left(\frac{3}{7}\right) = \left(\frac{3}{17}\right)$ but $\left(\frac{19}{7}\right) \ne \left(\frac{19}{17}\right)$, we observe that either $19 \mid a_i$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$ and $a_i \in \{1, 2, 3, 6\}$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$, or $19 \mid a_i$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$ and $a_i \in \{1, 2, 3, 6\}$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$. From $\psi = 2$, we obtain either $|\mathcal{I}_1| \le 3$ or $|\mathcal{I}_2| \le 3$, giving

$\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \le 3$. We find that $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \ge 4$ except when $i_{17} = 2$, in which case $\mathcal{I}_1 = \{6, 9, 15\}$ and $\mathcal{I}_2 = \{0, 3, 8, 13\}$. Now we see that $10 \notin \mathcal{M}$ and therefore there are at least two elements $i \in \mathcal{I}_1$ with $19 \,|\, a_i$. This is not possible. The cases $(i_{11}, i_{13}) \in \{(2, 4), (3, 5), (4, 0)\}$ are excluded similarly.

Let $(i_{11}, i_{13}) = (6, 2)$. As in the above case, we obtain $\mathcal{M}^k = \{8, 11, 13, 18\}$, $\mathcal{B}^k = \{0, 1, 3, 4, 5, 7, 9, 10, 12, 14, 16\}$, $i_5 = 3$, $7 \,|\, a_i$ for $i \in \{0, 7, 14\}$ and $i_{17} \in \{3, 11\}$. Further, $i_{17} = 3$ if $11 \notin \mathcal{M}$. For these choices of i_7, i_{17}, we take $p_1 = 7$, $p_2 = 17$ and $\mathcal{I} = \mathcal{B}^k$ to compute $\mathcal{I}_1$ and $\mathcal{I}_2$. We see from $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \le 3$ that $i_{17} = 11$, $\mathcal{I}_1 = \{5, 9\}$ and $\mathcal{I}_2 = \{1, 3, 4, 10, 12, 16\}$. If $\mathcal{I}_2 \subseteq \mathcal{B}$, then $t - |R| \ge 2$. Hence we may suppose that $i_{19} \in \{5, 9\}$, the other one is deleted and exactly one of $i \in \mathcal{I}_2$ is deleted. By reducing modulo 7, we see that either $a_i \in \{1, 2\}$ for $i \in \{1, 4, 16\} \cap \mathcal{B}$ and $a_i \in \{3, 6\}$ for $i \in \{3, 10, 12\} \cap \mathcal{B}$, or $a_i \in \{1, 2\}$ for $i \in \{3, 10, 12\} \cap \mathcal{B}$ and $a_i \in \{3, 6\}$ for $i \in \{1, 4, 16\} \cap \mathcal{B}$. If $a_i \in \{3, 6\}$ for $i \in \{3, 10, 12\} \cap \mathcal{B}$, then $10 \notin \mathcal{B}$ and $\left(\frac{a_i}{3}\right) = \left(\frac{d}{3}\right)$ for $i \in \{1, 4, 16\}$, giving $a_1 = a_4 = a_{16}$ and hence $t - |R| \ge 2$. Thus $a_i \in \{1, 2\}$ for $i \in \{3, 10, 12\} \cap \mathcal{B}$, and $a_i \in \{3, 6\}$ for $i \in \{1, 4, 16\} \cap \mathcal{B}$. By reducing modulo 5, we get $a_1 = a_{16} = 3$ if $1, 16 \in \mathcal{B}$, and by reducing modulo 3, we get $a_3 = a_{12} = 1$ if $3, 12 \in \mathcal{B}$. Since $|\mathcal{I}_2 \cap \mathcal{B}| = 5$ and $t - |R| \le 1$, we obtain

$$a_3 = a_{12} = 1, \quad a_{10} = 2, \quad a_4 = 6, \quad \text{either } a_1 = 3 \text{ or } a_{16} = 3 \tag{4.9}$$

or

$$a_1 = a_{16} = 3, \quad a_4 = 6, \quad a_{10} = 2, \quad \text{either } a_3 = 1 \text{ or } a_{12} = 1. \tag{4.10}$$

In the case $(i_{11}, i_{13}) = (1, 3)$, we obtain

$$a_6 = a_{15} = 1, \quad a_8 = 2, \quad a_{14} = 6, \quad \text{either } a_2 = 3 \text{ or } a_{17} = 3 \tag{4.11}$$

or

$$a_2 = a_{17} = 3, \quad a_{14} = 6, \quad a_8 = 2, \quad \text{either } a_6 = 1 \text{ or } a_{15} = 1. \tag{4.12}$$

As in [MuSh03], the possibilities (4.9), (4.11) are excluded by Runge's method and (4.10), (4.12) by Baker–Davenport's method on simultaneous Pell's equations.

4.4. *The case $k = 23$.* We may assume that $\sigma'_{23} = 1$ and $23 \nmid a_i$ for $0 \le i \le 3$ and $19 \le i < 23$, as otherwise the assertion follows from the case $k = 19$. We have $\sigma'_{11} = 3$ if $11 \,|\, a_{11j}$ with $j = 0, 1, 2$, and $\sigma'_{11} \le 2$ if $11 \nmid a_0 a_{11} a_{22}$. Also $\sigma'_7 = 4$ implies that $7 \,|\, a_{7j}$ or $7 \,|\, a_{1+7j}$ with $0 \le j \le 3$, and $\sigma'_7 \le 3$ otherwise. Thus $|\{a_i : 7 \,|\, a_i \text{ or } 11 \,|\, a_i\}| \le 6$. Further, by Euler's result for $k = 4$, we obtain $|\{a_i : P(a_i) = 5\}| \le 4$. If

$$|\{a_i : p \,|\, a_i,\ 5 \le p \le 23\} \le 4 + \sum_{7 \le p \le 23} \sigma_p - 1 - 2 = 15,$$

then from (2.10) with $r=2$ we get $t-|R|\geq k-2-15-4=2$, a contradiction. Therefore we have

$$(4.13)\qquad 4+\sum_{7\leq p\leq 23}\sigma_p-2\leq |\{a_i : p\,|\,a_i, 5\leq p\leq 23\}|\leq 4+\sum_{7\leq p\leq 19}\sigma_p-1.$$

Let $p_1=11$, $p_2=13$ and $\mathcal{I}=\{\gamma_1,\ldots,\gamma_t\}$. Then as in the case $k=19$, we observe that for $i\in\mathcal{M}$, exactly one of $5\,|\,a_i$ or $17\,|\,a_i$ holds but $5\cdot 17\nmid a_i$. Further, for $i\in\mathcal{B}$, either $5\nmid a_i$ and $17\nmid a_i$, or $5\cdot 17\,|\,a_i$. Since $\sigma_5\leq 5$ and $\sigma_{17}\leq 2$, we obtain $|\mathcal{M}^k|\leq 9$ and $5\,|\,a_i$ for at least $|\mathcal{M}^k|-4$ i's with $i\in\mathcal{M}^k$.

By taking the mirror image (4.4) of (1.1), we may suppose that $0\leq i_{11}<11$ and $0\leq i_{13}\leq 11$. For each of these pairs (i_{11},i_{13}), we compute $|\mathcal{I}_1^k|,|\mathcal{I}_2^k|$ and check that $\max(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)>9$. First we restrict to those pairs (i_{11},i_{13}) for which $\min(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\leq 9$. Therefore $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality, and hence $\mathcal{B}^k$ is the other set. Now we restrict to those pairs (i_{11},i_{13}) for which there are at least $|\mathcal{M}^k|-2$ elements $i\in\mathcal{M}^k$ such that either $5\,|\,a_i$ or $17\,|\,a_i$. There are 31 such pairs. Next we count the number of multiples of $11,13$, maximum multiples of $5,17$ in $\mathcal{M}^k\cup\mathcal{B}^k$ and $7,19$ in $\mathcal{B}^k$ to check that (4.13) is not valid. This is a contradiction.

For example, let $(i_{11},i_{13})=(0,2)$. Then $\mathcal{M}^k=\{4,6,9,18,19,20\}$ and $\mathcal{B}^k=\{1,3,5,7,8,10,12,13,14,16,17,21\}$, giving $5\,|\,a_i$ for $i\in\{4,9,19\}$, $i_5=4$. Further, $17\,|\,a_i$ for exactly one $i\in\{6,18,20\}$ and the other two i's in $\{6,18,20\}$ are deleted. Thus $5\cdot 17\nmid a_{14}$ so that (4.13) is not valid. For another example, let $(i_{11},i_{13})=(4,0)$. Then $\mathcal{M}^k=\{6,9,11,16,21\}$ and $\mathcal{B}^k=\{1,2,3,5,7,8,10,12,14,17,18,19,20,22\}$, giving $5\,|\,a_i$ for $i\in\{6,11,16,21\}$, $i_5=1$. Further, we have either $17\,|\,a_9$ and $\gcd(5\cdot 17,a_1)=1$, or $9\notin\mathcal{M}$ and $5\cdot 17\,|\,a_1$. Now $7\,|\,a_i$ for at most three elements $i\in\mathcal{B}^k$ so that (4.13) is not satisfied. This is a contradiction.

4.5. *The case $k=31$.* From $t-|R|\geq k-2-\sum_{7\leq p\leq 31}\sigma'_p-8\geq k-2-\sum_{7\leq p\leq 31}\sigma_p-8=1$ by (2.10) and (2.13) with $r=3$, we may assume for each prime $7\leq p\leq 31$ that $\sigma'_p=\sigma_p$ and for any i, $pq\nmid a_i$ whenever $7\leq p<q\leq 31$. Let $\mathcal{I}=\{\gamma_1,\ldots,\gamma_t\}$. By taking the mirror image (4.4) of (1.1) and $\sigma_{19}=\sigma_{29}=2$, we may assume that $i_{29}=0$ and $1\leq i_{19}\leq 11$, $i_{19}\neq 10$. For $p\leq 31$ with $p\neq 19,29$, since $\left(\frac{p}{19}\right)\neq\left(\frac{p}{29}\right)$ if and only if $p=11,13,17$, we observe that for $i\in\mathcal{M}$, either $11\,|\,a_i$ or $13\,|\,a_i$ or $17\,|\,a_i$. Since $\sigma_{11}+\sigma_{13}+\sigma_{17}\leq 8$, we obtain $|\mathcal{M}^k|\leq 10$ and $p\,|\,a_i$ for at least $|\mathcal{M}^k|-2$ elements $i\in\mathcal{M}^k$ and $p\in\{11,13,17\}$. Now for each pair (i_{19},i_{29}) given by $i_{29}=0$, $1\leq i_{19}\leq 11$, $i_{19}\neq 10$, we compute $|\mathcal{I}_1^k|,|\mathcal{I}_2^k|$. Since $\max(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\geq 14$, we restrict to those pairs (i_{19},i_{29}) with $\min(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\leq 10$. Then we are left with the only pair $(i_{19},i_{29})=(1,0)$. Further, noticing that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality, we get $\mathcal{M}^k=\{3,5,6,7,11,14,15,19,24,25\}$ and $\mathcal{B}^k=\{2,4,8,9,10,12,13,16,17,18,21,22,23,26,27,28,30\}$. We find that

there are at most seven elements $i \in \mathcal{M}^k$ for which either $11 \mid a_i$ or $13 \mid a_i$ or $17 \mid a_i$. This is not possible. ∎

References

[Dus99] P. Dusart, *Inégalités explicites pour $\psi(X), \theta(X), \pi(X)$ et les nombres premiers*, C. R. Math. Rep. Acad. Sci. Canada 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.

[HiLaShTi07] N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman, *An extension of a theorem of Euler*, Acta Arith. 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.

[LaSh07] —, —, *The equation $n(n+d)\cdots(n+(k-1)d) = by^2$ with $\omega(d) \le 6$ or $d \le 10^{10}$*, Acta Arith. 129 (2007), 249–305.

[MuSh03] A. Mukhopadhyay and T. N. Shorey, *Almost squares in arithmetic progression (II)*, ibid. 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.

[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., 113–124.

[ShTi90] T. N. Shorey and R. Tijdeman, *Perfect powers in products of terms in an arithmetical progression*, ibid. 75 (1990), 307–344.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: slaishram@math.uwaterloo.ca

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai, 400 005, India
E-mail: shorey@math.tifr.res.in

Received on 22.1.2007
and in revised form on 6.5.2008 (5374)