ACTA ARITHMETICA
129.1 (2007)

An extension of a theorem of Euler

by

NORIKO HIRATA-KOHNO (Tokyo), SHANTA LAISHRAM (Mumbai),
T. N. SHOREY (Mumbai), and R. TIJDEMAN (Leiden)

1. Introduction. The theorem of Euler ([Eul80], cf. [Mor69, pp. 21–22], [MS03]) referred to in the title of this paper is that a product of four terms in arithmetic progression is never a square. Let $n, d, k \geq 2$ and y be positive integers such that $\gcd(n, d) = 1$. We consider the equation

$$n(n+d)\cdots(n+(k-1)d) = y^2 \tag{1}$$

in n, d, k and y. It has infinitely many solutions when $k = 2$ or 3. A well-known conjecture states that (1) with $k \geq 4$ is not possible. We claim

THEOREM 1. *Equation* (1) *with* $4 \leq k \leq 109$ *is not possible.*

By Euler, Theorem 1 is valid when $k = 4$. The case when $k = 5$ is due to Obláth [Obl50]. Independently of the authors, Bennett, Bruin, Győry and Hajdu [BBGH06] proved that (1) with $6 \leq k \leq 11$ does not hold. Theorem 1 has been confirmed by Erdős [Erd39] and Rigge [Rig39], independently of each other, when $d = 1$.

Theorem 1 is derived from a more general result and we introduce some notation for stating this. For an integer $\nu > 1$, we denote by $P(\nu)$ the greatest prime factor of ν and we put $P(1) = 1$. Let b be a squarefree positive integer such that $P(b) \leq k$. We consider a more general equation than (1), namely

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

We write

$$n + id = a_i x_i^2 \quad \text{for } 0 \leq i < k \tag{3}$$

where a_i are squarefree integers such that $P(a_i) \leq \max(P(b), k-1)$ and x_i are positive integers. Every solution to (2) yields a k-tuple $(a_0, a_1, \ldots, a_{k-1})$. We rewrite (2) as

$$m(m-d)\cdots(m-(k-1)d) = by^2, \quad m = n + (k-1)d. \tag{4}$$

2000 *Mathematics Subject Classification*: Primary 11D61.
Key words and phrases: Euler, Diophantine equations, squares, Legendre symbol.

Equation (4) is called the *mirror image* of (2). The corresponding k-tuple $(a_{k-1}, a_{k-2}, \dots, a_0)$ is called the *mirror image* of $(a_0, a_1, \dots, a_{k-1})$.

Let $P(b) < k$. Erdős and Selfridge [ES75] proved that (2) with $d = 1$ never holds under the assumption that the left-hand side of (2) is divisible by a prime greater than or equal to k. The result does not hold unconditionally. As mentioned above, equation (2) with $k = 2, 3$ and $b = 1$ has infinitely many solutions. This is also the case when $k = 4$ and $b = 6$; see Tijdeman [Tij89]. On the other hand, equation (2) with $k = 4$ and $b \neq 6$ does not hold. We consider (2) with $d > 1$ and $k \geq 5$. We prove

THEOREM 2. *Equation* (2) *with* $d > 1$, $P(b) < k$ *and* $5 \leq k \leq 100$ *implies that* $(a_0, a_1, \dots, a_{k-1})$ *is among the following tuples or their mirror images*:

$$\begin{aligned} &k = 8: && (2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10);\\ &k = 9: && (2,3,1,5,6,7,2,1,10);\\ &k = 14: && (3,1,5,6,7,2,1,10,11,3,13,14,15,1);\\ &k = 24: && (5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3,7). \end{aligned} \tag{5}$$

Theorem 2 with $k = 5$ is due to Mukhopadhyay and Shorey [MS03]. Initially, Bennett, Bruin, Győry, Hajdu [BBGH06] and Hirata-Kohno, Shorey (unpublished), independently, proved Theorem 2 with $k = 6$ and $(a_0, a_1, \dots, a_5) \neq (1,2,3,1,5,6), (6,5,1,3,2,1)$. Next, Bennett, Bruin, Győry and Hajdu [BBGH06] removed the assumption on $(a_0, a_1, \dots, a_5)$ in the above result. Thus (2) with $k = 6$ does not hold and we shall refer to it as *the case* $k = 6$. Bennett, Bruin, Győry and Hajdu [BBGH06], independently of us, showed that (2) with $7 \leq k \leq 11$ and $P(b) \leq 5$ is not possible. This is now a special case of Theorem 2.

Let $P(b) = k$. Then we have no new result on (2) with $k = 5$. For $k \geq 7$, we prove

THEOREM 3. *Equation* (2) *with* $d > 1$, $P(b) = k$ *and* $7 \leq k \leq 100$ *implies that* $(a_0, a_1, \dots, a_{k-1})$ *is among the following tuples or their mirror images*:

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

It has been conjectured that (2) with $k \geq 5$ never holds. Granville (unpublished) showed that k is bounded by an absolute constant whenever the *abc*-conjecture holds; see Laishram [Lai04] for a proof. For the convenience of the proofs, we consider Theorems 2 and 3 together. Therefore we formulate

THEOREM 4. *Let $d > 1, P(b) \leq k$ and $5 \leq k \leq 100$. Suppose that $k \neq 5$ if $P(b) = k$. Then* (2) *does not hold except for the* $(a_0, a_1, \dots, a_{k-1})$ *among* (5), (6) *and their mirror images.*

It is clear that Theorem 4 implies Theorems 2 and 3. In fact the proof of Theorem 4 provides a method for solving (2) for any given value of k unless $(a_0, a_1, \dots, a_{k-1})$ is given by (5), (6) and their mirror images. This is a new and useful feature of the paper. We have restricted k up to 100 for keeping the computational load under control. It is an open problem to solve (2) for an infinite sequence of values of k. A solution to this problem may be an important contribution towards the conjecture stated just after Theorem 3. Theorem 4 has been applied in [LS] to show that (2) with $k \geq 6$ implies that $d > 10^{10}$. For more applications, see [LS].

Now we give a sketch of the proof of Theorem 4. Let the assumptions of Theorem 4 be satisfied. Assume (2) such that $(a_0, a_1, \dots, a_{k-1})$ is not among (5), (6) or their mirror images. As already stated, the cases $k = 5$ and $k = 6$ have already been solved in [MS03] and [BBGH06]. Therefore we suppose that $k \geq 7$. Further it suffices to assume that k is prime and we proceed inductively on k. Let k be given. Then we choose a suitable pair (q_1, q_2) of distinct primes $\leq k$ such that

$$\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right)$$

for small primes p. For example, when $k = 29$, we take $(q_1, q_2) = (19, 29)$ so that the above relation holds with $p = 2, 3, 5, 7$. We show that $q_1 \nmid d$ and $q_2 \nmid d$ (see Lemma 8). Assume $q_1 \mid d$ or $q_2 \mid d$. Then we find two primes Q_1 and Q_2 such that $Q_1 \mid d$ or $Q_2 \mid d$ whenever $k \geq 29$ (see Lemma 7). Now we arrive at a contradiction by a counting argument using (9) and Lemmas 1, 2. Hence $q_1 \nmid d$ and $q_2 \nmid d$ but this is excluded by Lemma 6, the proof of which depends on Lemma 5. In fact, we need to apply it repeatedly for $k > 11$.

In the case $k = 6$, Bennett, Bruin, Győry and Hajdu [BBGH06] solved the cases $(a_0, a_1, \dots, a_5) \in \{(1, 2, 3, 1, 5, 6), (6, 5, 1, 3, 2, 1)\}$ by using explicit Chabauty techniques due to Bruin and Flynn [BF05]. These cases appear to be similar to our exceptional cases (5) and (6) where we have, in fact, more freedom in the sense that there are at least 7 curves where we may consider applying the Chabauty method. Finally we remark that it suffices to solve the cases $k = 7$ in (6) or its mirror images for Theorem 3 and the cases $k = 8$ in (5) or its mirror images for Theorem 2.

2. Notation and lemmas.

We introduce some notation. Let

$$R = \{a_i : 0 \leq i < k\}$$

and, for a prime q, put

$$S = S(q) = \{a \in R : P(a) \le q\}, \quad S_1 = S_1(q) = \{a \in R : P(a) > q\}. \tag{7}$$

Further we write

$$T = T(q) = \{i : a_i \in S\}, \quad T_1 = T_1(q) = \{i : a_i \in S_1\}. \tag{8}$$

Then we see that

$$|T| + |T_1| = k. \tag{9}$$

For $a \in R$, let

$$\nu(a) = |\{i : a_i = a\}|,$$
$$\nu_{\mathrm{o}}(a) = |\{i : a_i = a,\, 2 \nmid x_i\}|, \quad \nu_{\mathrm{e}}(a) = |\{i : a_i = a,\, 2 \mid x_i\}|.$$

We observe that

$$|T| = \sum_{a \in S} \nu(a). \tag{10}$$

Let

$$\delta = \min(3, \mathrm{ord}_2(d)), \quad \varrho = \begin{cases} 3 & \text{if } 3 \mid d, \\ 1 & \text{otherwise.} \end{cases}$$

We have

Lemma 1. *For $a \in R$, let $\mathcal{K}_a = k/a2^{3-\delta}$, $\mathcal{K}'_a = k/16a$,*

$$f_1(k,a,\delta) = \begin{cases} 1 & \text{if } k \le a2^{3-\delta}, \\ \lceil \mathcal{K}_a \rceil - \left[\dfrac{\lceil \mathcal{K}_a \rceil}{4} \right] & \text{if } k > a2^{3-\delta},\ 3 \mid d, \\ \displaystyle\sum_{i=1}^{2} \left(\left\lceil \frac{\mathcal{K}_a}{3^i} \right\rceil - \left[\frac{\lceil \mathcal{K}_a/3^i \rceil}{4} \right] \right) & \text{if } k > a2^{3-\delta},\ 3 \nmid d, \end{cases}$$

and

$$f_2(k,a) = \begin{cases} 1 & \text{if } k \le 4a, \\ \lceil \mathcal{K}'_a \rceil + 1 & \text{if } 4a < k \le 32a, \\ \displaystyle\sum_{i=1}^{2} \left(\left\lceil \frac{\mathcal{K}'_a}{i} \right\rceil - \left[\frac{\lceil \mathcal{K}'_a/i \rceil}{4} \right] \right) & \text{if } k > 32a,\ 3 \mid d, \\ \displaystyle\sum_{i=1}^{2} \left(\left\lceil \frac{\mathcal{K}'_a}{3^i} \right\rceil - \left[\frac{\lceil \mathcal{K}'_a/3^i \rceil}{4} \right] \right) + \sum_{i=1}^{2} \left(\left\lceil \frac{\mathcal{K}'_a}{2 \cdot 3^i} \right\rceil - \left[\frac{\lceil \mathcal{K}'_a/2 \cdot 3^i \rceil}{4} \right] \right) & \\ & \text{if } k > 32a,\ 3 \nmid d. \end{cases}$$

Then we have

$$\nu_{\mathrm{o}}(a) \le f_1(k,a,\delta), \quad \nu_{\mathrm{e}}(a) \le f_2(k,a),$$

and

$$\nu(a) \le F(k,a,\delta) := \begin{cases} 1 & \textit{if } k \le a, \\ f_1(k,a,\delta) & \textit{if } k > a \textit{ and } d \textit{ even}, \\ f_1(k,a,0) + f_2(k,a) & \textit{if } k > a \textit{ and } d \textit{ odd.} \end{cases}$$

Proof. Let $I_1 = \{i : a_i = a,\, x_i \text{ odd}\}$, $I_2 = \{i : a_i = a,\, 2 \,\|\, x_i\}$ and $I_3 = \{i : a_i = a,\, 4 \mid x_i\}$. Further, for $l = 1,2,3$, let

$$I_{l1} := \{i \in I_l : 3 \nmid x_i\}, \qquad I_{l2} := \{i \in I_l : 3 \mid x_i\}.$$

Let $\tau := \tau(l,m)$ be defined by $\tau/a = 2^{3-\delta}\cdot 3\varrho^{-1}$, $2^{3-\delta}\cdot 9$, $32\cdot 3\varrho^{-1}$, $32\cdot 9$, $16\cdot 3\varrho^{-1}$, $16\cdot 9$ for $(l,m) = (1,1),(1,2),(2,1),(2,2),(3,1),(3,2)$, respectively. Since $x_i^2 \equiv 1 \pmod 8$ for $i \in I_1$, $(x_i/2)^2 \equiv 1 \pmod 8$ for $i \in I_2$, $16 \mid x_i^2$ for $i \in I_3$ and $x_i^2 \equiv 1 \pmod 3$ for $i \in I_{l1}$, $9 \mid x_i^2$ for $i \in I_{l2}$ for $l = 1,2,3$, we see from $(i-j)d = a(x_i^2 - x_j^2)$ that $\tau \mid i - j$ for $i,j \in I_{lm}$. Since $a \mid i - j$ whenever $a_i = a_j$, we get $\nu(a) = 1$ for $k \le a$. Thus we suppose that $k > a$. We have $\nu(a) = \nu_{\mathrm{o}}(a) + \nu_{\mathrm{e}}(a)$. It suffices to show $\nu_{\mathrm{o}}(a) \le f_1(k,a,\delta)$ and $\nu_{\mathrm{e}}(a) \le f_2(k,a)$ since $\nu_{\mathrm{e}}(a) = 0$ for d even. We observe that $\nu_{\mathrm{o}}(a) = |I_1|$ and $\nu_{\mathrm{e}}(a) = |I_2| + |I_3|$. Since $a2^{3-\delta} \mid i - j$ whenever $i,j \in I_1$, we get $|I_1| \le 1$ if $k \le a2^{3-\delta}$. Thus we suppose $k > a2^{3-\delta}$ for proving $|I_1| \le f_1(k,a,\delta)$. Further from $4a \mid i - j$ for $i,j \in I_2 \cup I_3$, $32a \mid i - j$ for $i,j \in I_2$ and $16a \mid i - j$ for $i,j \in I_3$, we get $|I_2| + |I_3| \le f_2(k,a)$ for $k \le 32a$. Hence we suppose that $k > 32a$ for showing $|I_2| + |I_3| \le f_2(k,a)$.

Let (l,m) have $1 \le l \le 3$, $1 \le m \le 2$. Let $i_0 = \min_{i \in I_{lm}} i$, $N = (n + i_0 d)/a$ and $D = \tau d/a$. Then we see that ax_i^2 with $i \in I_{lm}$ come from the squares in the set $\{N, N + D, \ldots, N + (\lceil (k - i_0)/\tau \rceil - 1)D\}$. Dividing this set into consecutive intervals of length 4 and using Euler's result, we see that there are at most

$$\left\lceil \frac{k - i_0}{\tau} \right\rceil - \left[\frac{\lceil (k - i_0)/\tau \rceil}{4} \right] \le \left\lceil \frac{k}{\tau} \right\rceil - \left[\frac{\lceil k/\tau \rceil}{4} \right]$$

of them which can be squares. Hence $|I_{lm}| \le \lceil k/\tau \rceil - [\lceil k/\tau \rceil/4]$. Now the assertion follows from $|I_l| = \sum_{m=1}^{2} |I_{lm}|$ for $l = 1,2,3$ since $|I_{l2}| = 0$ for $3 \mid d$. ∎

We observe that there are $(p-1)/2$ distinct quadratic residues and $(p-1)/2$ distinct quadratic nonresidues modulo an odd prime p. The next lemma follows easily from this fact.

Lemma 2. *Assume* (2) *holds. Let k be an odd prime. Suppose that $k \nmid d$. Let*

$$T' = \left\{ i : \left(\frac{a_i}{k} \right) = 1,\, 0 \le i < k \right\}, \qquad T'' = \left\{ i : \left(\frac{a_i}{k} \right) = -1,\, 0 \le i < k \right\}.$$

Then

$$|T'| = |T''| = \frac{k-1}{2}.$$

LEMMA 3. *Assume that* (2) *with* $P(b) \le k$ *has no solution at* $k = k_1$ *with* k_1 *prime. Then* (2) *with* $P(b) \le k$ *has no solution at* k *with* $k_1 \le k < k_2$, *where* k_2 *is the smallest prime larger than* k_1.

Proof. Let k_1 and k_2 be consecutive primes such that $k_1 \le k < k_2$. Assume that (2) does not hold at (n, d, k_1). Suppose

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

Using (3), we see that

$$n(n+d)\cdots(n+(k_1-1)d) = b'y'^2$$

with $P(b') \le k_1$. This is not possible. ■

Let q_1, q_2 be distinct primes and

$$\Lambda_1(q_1,q_2) := \left\{p \le 97 : \left(\frac{p}{q_1}\right) \ne \left(\frac{p}{q_2}\right)\right\}.$$

We write $\Lambda(q_1,q_2) = \Lambda(q_1,q_2,k) := \{p \in \Lambda_1(q_1,q_2) : p \le k\}$.

LEMMA 4. *We have*

(q_1,q_2)	$\Lambda_1(q_1,q_2)$
$(5,11)$	$\{3,19,23,29,37,41,47,53,61,67,79,97\}$
$(7,17)$	$\{11,13,19,23,29,37,47,59,71,79,83,89\}$
$(11,13)$	$\{5,17,29,31,37,43,47,59,61,67,71,79,89,97\}$
$(11,59)$	$\{7,17,19,23,29,31,37,41,47,67,79,89,97\}$
$(11,61)$	$\{13,19,23,31,37,41,53,59,67,71,73,83,89\}$
$(19,29)$	$\{11,13,17,43,47,53,59,61,67,71,73\}$
$(23,73)$	$\{13,19,29,31,37,47,59,61,67,79,89,97\}$
$(23,97)$	$\{11,13,29,41,43,53,59,61,71,79,89\}$
$(31,89)$	$\{7,11,17,19,41,53,59,73,79\}$
$(37,83)$	$\{17,23,29,31,47,53,59,61,67,71,73\}$
$(41,79)$	$\{11,13,19,37,43,59,61,67,89,97\}$
$(43,53)$	$\{7,23,29,31,37,41,67,79,83,89\}$
$(43,67)$	$\{11,13,19,29,31,37,41,53,71,73,79,89,97\}$
$(53,67)$	$\{7,11,13,19,23,43,71,73,83,97\}$
$(59,61)$	$\{7,13,17,29,47,53,71,73,79,83,97\}$
$(73,97)$	$\{11,19,23,31,37,41,43,47,53,67,71\}$
$(79,89)$	$\{13,17,19,23,31,47,53,71,83\}$

Definition. Let $\mathcal{P}$ be a set of primes and $\mathcal{I} \subseteq [0,k) \cap \mathbb{Z}$. We say that $\mathcal{I}$ is *covered* by $\mathcal{P}$ if, for every $j \in \mathcal{I}$, there exists $p \in \mathcal{P}$ such that $p \mid a_j$. Further, for $i \in \mathcal{I}$, let

$$\mathfrak{i}(\mathcal{P}) = |\{p \in \mathcal{P} : p \text{ divides } a_i\}|. \tag{11}$$

For a prime p with $\gcd(p,d) = 1$, let i_p be the smallest $i \geq 0$ such that $p \mid n + id$. For $\mathcal{I} \subseteq [0,k) \cap \mathbb{Z}$ and primes p_1, p_2 with $\gcd(p_1p_2, d) = 1$, we write

$$\mathcal{I}' = \mathcal{I}(p_1, p_2) = \mathcal{I} \setminus \bigcup_{j=1}^{2} \{i_{p_j} + p_j i : 0 \leq i < \lceil k/p_j \rceil\}.$$

Lemma 5. *Let $\mathcal{P}_0$ be a set of primes. Let p_1, p_2 be primes such that $\gcd(p_1p_2, d) = 1$. Let $(i_1, i_2) = (i_{p_1}, i_{p_2})$, $\mathcal{I} \subseteq [0,k) \cap \mathbb{Z}$ and $\mathcal{I}' = \mathcal{I}(p_1, p_2)$ be such that $\mathfrak{i}(\mathcal{P}_0 \cap \Lambda(p_1, p_2))$ is even for each $i \in \mathcal{I}'$. Define*

$$\mathcal{I}_1 = \left\{ i \in \mathcal{I}' : \left(\frac{i - i_1}{p_1}\right) = \left(\frac{i - i_2}{p_2}\right) \right\},$$
$$\mathcal{I}_2 = \left\{ i \in \mathcal{I}' : \left(\frac{i - i_1}{p_1}\right) \neq \left(\frac{i - i_2}{p_2}\right) \right\}.$$

Let $\mathcal{P} = \Lambda(p_1, p_2) \setminus \mathcal{P}_0$. Let ℓ be the number of terms $n + id$ with $i \in \mathcal{I}'$ divisible by primes in $\mathcal{P}$. Then either

$$|\mathcal{I}_1| \leq \ell, \quad \mathcal{I}_1 \text{ is covered by } \mathcal{P}, \quad \mathcal{I}_2 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is even}\},$$

or

$$|\mathcal{I}_2| \leq \ell, \quad \mathcal{I}_2 \text{ is covered by } \mathcal{P}, \quad \mathcal{I}_1 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is even}\}.$$

We observe that $\ell \leq \sum_{p \in \mathcal{P}} \lceil k/p \rceil$.

Proof. Let $i \in \mathcal{I}'$. Let $\mathcal{U}_0 = \{p : p \mid a_i\}$, $\mathcal{U}_1 = \{p \in \mathcal{U}_0 : p \notin \Lambda(p_1, p_2)\}$, $\mathcal{U}_2 = \{p \in \mathcal{U}_0 : p \in \mathcal{P}_0 \cap \Lambda(p_1, p_2)\}$ and $\mathcal{U}_3 = \{p \in \mathcal{U}_0 : p \in \mathcal{P}\}$. Then we deduce from $a_i = \prod_{p \in \mathcal{U}_0} p$ that

$$\left(\frac{a_i}{p_1}\right) = \prod_{p \in \mathcal{U}_1} \left(\frac{p}{p_1}\right) \prod_{p \in \mathcal{U}_2} \left(\frac{p}{p_1}\right) \prod_{p \in \mathcal{U}_3} \left(\frac{p}{p_1}\right) = (-1)^{\mathfrak{i}(\mathcal{P}) + |\mathcal{U}_2|} \prod_{p \in \mathcal{U}_0} \left(\frac{p}{p_2}\right)$$
$$= (-1)^{\mathfrak{i}(\mathcal{P})} \left(\frac{a_i}{p_2}\right)$$

since $|\mathcal{U}_2| = \mathfrak{i}(\mathcal{P}_0 \cap \Lambda(p_1, p_2))$ is even. Therefore

$$\mathcal{L} := \left\{ i \in \mathcal{I}' : \left(\frac{a_i}{p_1}\right) \neq \left(\frac{a_i}{p_2}\right) \right\} = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is odd}\}. \tag{12}$$

In particular, $\mathcal{L}$ is covered by $\mathcal{P}$ and hence

$$|\mathcal{L}| \leq \ell. \tag{13}$$

We see that $\left(\frac{a_i}{p_j}\right) = \left(\frac{n+id}{p_j}\right) = \left(\frac{i-i_j}{p_j}\right)\left(\frac{d}{p_j}\right)$ for $i \in \mathcal{I}'$ and $j = 1, 2$. Therefore $\mathcal{L} = \mathcal{I}_1$ or $\mathcal{I}_2$ according as $\left(\frac{d}{p_1}\right) \neq \left(\frac{d}{p_2}\right)$ or $\left(\frac{d}{p_1}\right) = \left(\frac{d}{p_2}\right)$, respectively. Now the assertion of Lemma 5 follows from (12) and (13). ∎

Remark. Let $\mathcal{P}$ consist of one prime p. We observe that $p \mid n+id$ if and only if $p \mid i - i_p$. Then $\mathcal{I}_1$ or $\mathcal{I}_2$ is contained in one residue class modulo p and $p \nmid a_i$ for i in the other set.

Corollary 1. *Let $p_1, p_2, i_1, i_2, \mathcal{P}_0, \mathcal{P}, \mathcal{I}, \mathcal{I}', \mathcal{I}_1, \mathcal{I}_2$ and ℓ be as in Lemma 5. Assume that*

$$\ell < \frac{1}{2}\,|\mathcal{I}'|. \tag{14}$$

Then $|\mathcal{I}_1| \neq |\mathcal{I}_2|$. Let

$$\mathcal{M} = \begin{cases} \mathcal{I}_1 & \textit{if } |\mathcal{I}_1| < |\mathcal{I}_2|, \\ \mathcal{I}_2 & \textit{otherwise}, \end{cases} \tag{15}$$

$$\mathcal{B} = \begin{cases} \mathcal{I}_2 & \textit{if } |\mathcal{I}_1| < |\mathcal{I}_2|, \\ \mathcal{I}_1 & \textit{otherwise.} \end{cases} \tag{16}$$

Then $|\mathcal{M}| \leq \ell$, $\mathcal{M}$ is covered by $\mathcal{P}$ and $\mathcal{B} = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P})$ is even$\}$.

Proof. We see from Lemma 5 that $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \leq \ell$ and from (14) that $\max(|\mathcal{I}_1|, |\mathcal{I}_2|) \geq \frac{1}{2}|\mathcal{I}'| > \ell$. Now the assertion follows from Lemma 5. ∎

We say that $(\mathcal{M}, \mathcal{B}, \mathcal{P}, \ell)$ has *Property* $\mathfrak{H}$ if $|\mathcal{M}| \leq \ell$, $\mathcal{M}$ is covered by $\mathcal{P}$ and $\mathfrak{i}(\mathcal{P})$ is even for $i \in \mathcal{B}$.

Lemma 6. *Let k be a prime with $7 \leq k \leq 97$ and assume* (2). *For $k \geq 11$, assume that Theorem* 4 *is valid for all primes k_1 with $7 \leq k_1 < k$. For $11 \leq k \leq 29$, assume that $k \nmid d$ and $k \nmid n + id$ for $0 \leq i < k - k'$ and $k' \leq i < k$ where $k' < k$ are consecutive primes. Let $(q_1, q_2) = (5, 7)$ if $k = 7$; $(5, 11)$ if $k = 11$; $(11, 13)$ if $13 \leq k \leq 23$; $(19, 29)$ if $29 \leq k \leq 59$; $(59, 61)$ if $k = 61$; $(43, 67)$ if $k = 67, 71$; $(23, 73)$ if $k = 73, 79$; $(37, 83)$ if $k = 83$; $(79, 89)$ if $k = 89$; and $(23, 97)$ if $k = 97$. Then $q_1 \mid d$ or $q_2 \mid d$ unless $(a_0, a_1, \ldots, a_{k-1})$ is given by the following tuples or their mirror images.*

$k = 7$: $(2, 3, 1, 5, 6, 7, 2), (3, 1, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, 1, 10)$;
$k = 13$: $(3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15), (1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1)$;
$k = 19$: $(1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22)$;
$k = 23$: $(5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3)$,
$(6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3, 7)$.

We shall prove Lemma 6 in Section 3.

Lemma 7. *Let k be a prime with $29 \leq k \leq 97$ and Q_0 a prime dividing d. Assume* (2) *with $k \nmid d$ and $k \nmid n + id$ for $0 \leq i < k - k'$ and $k' \leq i < k$ where $k' < k$ are consecutive primes. Then there are primes Q_1 and Q_2 given in the following table such that either $Q_1 \mid d$ or $Q_2 \mid d$:*

k	Q_0	(Q_1, Q_2)	k	Q_0	(Q_1, Q_2)
$29 \le k \le 59$	19	$(7, 17)$	$73, 79$	23	$(53, 67)$
$31 \le k \le 59$	29	$(7, 17)$	79	73	$(53, 67)$
61	59	$(11, 61)$	83	37	$(23, 73)$
$67, 71$	43	$(53, 67)$	89	79	$(23, 73)$
71	67	$(43, 53)$	97	23	$(73, 97), (37, 83)$

The proofs of Lemmas 6 and 7 depend on the repeated application of Lemma 5 and Corollary 1. We shall prove Lemma 7 in Section 4. Next we shall apply Lemmas 1, 2 and 7 to prove the following result.

LEMMA 8. *Let k be a prime with $7 \le k \le 97$. Assume* (2) *with $k \nmid d$. Further for $k \ge 29$, assume that $k \nmid n + id$ for $0 \le i < k - k'$ and $k' \le i < k$ where $k' < k$ are consecutive primes. Let (q_1, q_2) be as in Lemma* 6. *Then $q_1 \nmid d$ and $q_2 \nmid d$.*

Section 5 contains a proof of Lemma 8. Assume that $3 \nmid d$ and $5 \nmid d$. We define some more notation. For a subset $\mathcal{J} \subseteq [0, k) \cap \mathbb{Z}$, let

$$\mathcal{I}_3^0 = \mathcal{I}_3^0(\mathcal{J}) := \{i \in \mathcal{J} : i \equiv i_3 \ (\mathrm{mod}\, 3)\},$$

$$\mathcal{I}_3^+ = \mathcal{I}_3^+(\mathcal{J}) := \left\{i \in \mathcal{J} : \left(\frac{i - i_3}{3}\right) = 1\right\},$$

$$\mathcal{I}_3^- = \mathcal{I}_3^-(\mathcal{J}) := \left\{i \in \mathcal{J} : \left(\frac{i - i_3}{3}\right) = -1\right\}$$

and

$$\mathcal{I}_5^+ = \mathcal{I}_5^+(\mathcal{J}) := \left\{i \in \mathcal{J} : \left(\frac{i - i_5}{5}\right) = 1\right\},$$

$$\mathcal{I}_5^- = \mathcal{I}_5^-(\mathcal{J}) := \left\{i \in \mathcal{J} : \left(\frac{i - i_5}{5}\right) = -1\right\}.$$

Assume that $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{I}_3^+ \cup \mathcal{I}_3^-$. Then either $a_i \in \{1, 7\}$ for $i \in \mathcal{I}_3^+$, $a_i \in \{2, 14\}$ for $i \in \mathcal{I}_3^-$ or $a_i \in \{2, 14\}$ for $i \in \mathcal{I}_3^+$, $a_i \in \{1, 7\}$ for $i \in \mathcal{I}_3^-$. We define $(\mathcal{I}_3^1, \mathcal{I}_3^2) = (\mathcal{I}_3^+, \mathcal{I}_3^-)$ in the former case and $(\mathcal{I}_3^1, \mathcal{I}_3^2) = (\mathcal{I}_3^-, \mathcal{I}_3^+)$ in the latter. We observe that i's have the same parity whenever $a_i \in \{2, 14\}$. Thus if i's have the same parity in one of $\mathcal{I}_3^+$ or $\mathcal{I}_3^-$ but not in both, then we see that $(\mathcal{I}_3^1, \mathcal{I}_3^2) = (\mathcal{I}_3^+, \mathcal{I}_3^-)$ or $(\mathcal{I}_3^-, \mathcal{I}_3^+)$ according as i's have the same parity in $\mathcal{I}_3^-$ or $\mathcal{I}_3^+$, respectively. Further we write

$$\mathcal{J}_1 = \mathcal{I}_3^1 \cap \mathcal{I}_5^+, \quad \mathcal{J}_2 = \mathcal{I}_3^1 \cap \mathcal{I}_5^-, \quad \mathcal{J}_3 = \mathcal{I}_3^2 \cap \mathcal{I}_5^+, \quad \mathcal{J}_4 = \mathcal{I}_3^2 \cap \mathcal{I}_5^-$$

and $\mathfrak{a}_\mu = \{a_i : i \in \mathcal{J}_\mu\}$ for $1 \le \mu \le 4$. Since $\left(\frac{1}{5}\right) = \left(\frac{14}{5}\right) = 1$ and $\left(\frac{2}{5}\right) = \left(\frac{7}{5}\right) = -1$, we see that

$$(17) \qquad (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (\{1\}, \{7\}, \{14\}, \{2\}) \quad \text{or} \quad (\{7\}, \{1\}, \{2\}, \{14\})$$

where $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (S_1, S_2, S_3, S_4)$ denotes $\mathfrak{a}_\mu \subseteq S_\mu$, $1 \le \mu \le 4$. We use $7 \mid i - i'$ whenever $a_i, a_{i'} \in \{7, 14\}$ to exclude one of the above possibilities.

3. Proof of Lemma 6. Let $k' < k$ be consecutive primes. We may suppose that if (2) holds for some $k > 29$, then $k \nmid d$ and $k \nmid a_i$ for $0 \le i < k - k'$ and $k' \le i < k$, otherwise the assertion follows from Theorem 4 with k replaced by k'. Subsections 3.1 to 3.10 will be devoted to the proof of Lemma 6. We may assume that $q_1 \nmid d$ and $q_2 \nmid d$, otherwise the assertion follows.

3.1. *The case $k = 7$.* Then $5 \nmid d$. By taking the mirror images (4) of (2), there is no loss of generality in assuming that $5 \mid n + i_5 d$, $7 \mid n + i_7 d$ for some pair (i_5, i_7) with $0 \le i_5 < 5$, $0 \le i_7 \le 3$. Further we may suppose $i_7 \ge 1$, otherwise the assertion follows from the case $k = 6$. We apply Lemma 5 with $\mathcal{P}_0 = \emptyset$, $p_1 = 5$, $p_2 = 7$, $(i_1, i_2) = (i_5, i_7)$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \Lambda(5, 7) = \{2\}$ and $\ell \le \ell_1 = \lceil k/2 \rceil$ to conclude that either

$$|\mathcal{I}_1| \le \ell_1, \quad \mathcal{I}_1 \text{ is covered by } \mathcal{P}, \quad \mathcal{I}_2 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is even}\},$$

or

$$|\mathcal{I}_2| \le \ell_1, \quad \mathcal{I}_2 \text{ is covered by } \mathcal{P}, \quad \mathcal{I}_1 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is even}\}.$$

Let $(i_5, i_7) = (3, 1)$. Then $\mathcal{I}_1 = \{0, 2, 6\}$ and $\mathcal{I}_2 = \{4, 5\}$. We see that $\mathcal{I}_1$ is covered by $\mathcal{P}$ and hence $\mathfrak{i}(\mathcal{P})$ is even for $i \in \mathcal{I}_2$. Thus $2 \nmid a_i$ for $i \in \mathcal{I}_2$. Therefore $a_4, a_5 \in \{1, 3\}$ and $a_0, a_2, a_6 \in \{2, 6\}$. If $a_0 = 6$ or $a_6 = 6$, then $3 \nmid a_4 a_5$ so that $a_4 = a_5 = 1$. This is not possible by modulo 3. Thus $a_0 = a_6 = 2$. Since $\left(\frac{a_0}{5}\right)\left(\frac{a_2}{5}\right) = \left(\frac{(-3d)(-d)}{5}\right) = -1$, we get $a_2 = 6$. Hence $a_4 = 1$. Further $a_5 = 3$ since $\left(\frac{a_5}{5}\right)\left(\frac{a_4}{5}\right) = \left(\frac{(2d)(1d)}{5}\right) = -1$. Also $5 \mid a_3$ and $7 \mid a_1$, otherwise the assertion follows from the results of [MS03] for $k = 5$ and [BBGH06] for $k = 6$, respectively, stated in Section 1. In fact, $a_1 = 7$, $a_3 = 5$ by $\gcd(a_1 a_3, 6) = 1$. Thus $(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (2, 7, 6, 5, 1, 3, 2)$. The proofs for the other cases of (i_5, i_7) are similar. We get $(a_0, \ldots, a_6) = (1, 5, 6, 7, 2, 1, 10)$ when $(i_5, i_7) = (1, 3)$, $(a_0, \ldots, a_6) = (1, 2, 7, 6, 5, 1, 3)$ when $(i_5, i_7) = (4, 2)$ and all the other pairs are excluded. Hence Lemma 6 with $k = 7$ follows.

3.2. *The case $k = 11$.* Then $5 \nmid d$. By taking the mirror images (4) of (2), there is no loss of generality in assuming that $5 \mid n + i_5 d$, $11 \mid n + i_{11} d$ for some pair (i_5, i_{11}) with $0 \le i_5 < 5$, $4 \le i_{11} \le 5$. We apply Lemma 5 with $\mathcal{P}_0 = \emptyset$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) = (i_5, i_{11})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \Lambda(5, 11) = \{3\}$ and $\ell \le \ell_1 = \lceil k/3 \rceil$ to derive that either

$$|\mathcal{I}_1| \le \ell_1, \quad \mathcal{I}_1 \text{ is covered by } \mathcal{P}, \quad \mathcal{I}_2 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is even}\},$$

or

$$|\mathcal{I}_2| \le \ell_1, \quad \mathcal{I}_2 \text{ is covered by } \mathcal{P}, \quad \mathcal{I}_1 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is even}\}.$$

We compute $\mathcal{I}_1, \mathcal{I}_2$ and we restrict attention to those pairs (i_5, i_{11}) for which $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \le \ell_1$ and either $\mathcal{I}_1$ or $\mathcal{I}_2$ is covered by $\mathcal{P}$. We find that $(i_5, i_{11}) = (0,4), (1,5)$. Let $(i_5, i_{11}) = (0,4)$. Then $\mathcal{I}_1 = \{3, 9\}$ is covered by $\mathcal{P}$, $i_3 = 0$ and $\mathfrak{i}(\mathcal{P})$ is even for $i \in \mathcal{I}_2 = \{1,2,6,7,8\}$. Thus $3 \nmid a_i$ for $i \in \mathcal{I}_2$. Further, $p \in \{2,7\}$ whenever $p \mid a_i$ with $i \in \mathcal{I}_2$. Therefore $a_i \in \{1,2,7,14\}$ for $i \in \mathcal{I}_2$. By taking $\mathcal{J} = \mathcal{I}_2$, we have $\mathcal{I}_2 = \mathcal{I}_3^0 \cup \mathcal{I}_3^+ \cup \mathcal{I}_3^-$ and $\mathcal{I}_2 = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

$$\mathcal{I}_3^0 = \{6\}, \quad \mathcal{I}_3^+ = \{1,7\}, \quad \mathcal{I}_3^- = \{2,8\}, \quad \mathcal{I}_5^+ = \{1,6\}, \quad \mathcal{I}_5^- = \{2,7,8\}.$$

Let $(\mathcal{I}_3^1, \mathcal{I}_3^2) = (\mathcal{I}_3^+, \mathcal{I}_3^-)$. Then

$$\mathcal{J}_1 = \{1\}, \quad \mathcal{J}_2 = \{7\}, \quad \mathcal{J}_3 = \emptyset, \quad \mathcal{J}_4 = \{2,8\}.$$

The possibility $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (\{7\}, \{1\}, \{2\}, \{14\})$ is excluded since $7 \mid i - i'$ whenever $a_i, a_{i'} \in \{7, 14\}$. Therefore $a_1 = 1$, $a_7 = 7$, $a_2 = a_8 = 2$. Further, $a_6 = 1$ since $6 \in \mathcal{I}_5^+$ and $a_1 = 1$, $a_7 = 7$. This is not possible since $1 = \left(\frac{a_6}{7}\right)\left(\frac{a_8}{7}\right) = \left(\frac{(-d)(d)}{7}\right) = -1$. Let $(\mathcal{I}_3^1, \mathcal{I}_3^2) = (\mathcal{I}_3^-, \mathcal{I}_3^+)$. Then we argue as above to conclude that $a_2 = a_8 = 1$, $a_1 = 2$, $a_7 = 14$, which is not possible since $n + 2d$ and $n + 8d$ cannot both be odd squares. The other case $(i_5, i_{11}) = (1,5)$ is excluded similarly.

3.3. *The cases* $13 \le k \le 23$. Then $11 \nmid d$ and $13 \nmid d$. There is no loss of generality in assuming that $11 \mid n + i_{11}d$, $13 \mid n + i_{13}d$ for some pair (i_{11}, i_{13}) with $0 \le i_{11} < 11$, $0 \le i_{13} \le (k-1)/2$ and further $i_{13} \ge 2$ if $k = 13$. We have applied Lemma 5 once in each of cases $k = 7$ and $k = 11$ but we apply it twice for every case $13 \le k \le 23$ in this subsection. Let $\mathcal{P}_0 = \emptyset$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) = (i_{11}, i_{13})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \mathcal{P}_1 := \Lambda(11, 13)$ and $\ell \le \ell_1$ where $\ell_1 = 3$ if $k = 13$, and $\ell_1 = \lceil k/5 \rceil + \lceil k/17 \rceil$ if $k > 13$. Then $\ell_1 < \frac{1}{2}|\mathcal{I}'|$ since $|\mathcal{I}'| \ge k - \lceil k/11 \rceil - \lceil k/13 \rceil$. By Corollary 1, we derive that $\mathcal{I}'$ is partitioned into $\mathcal{M} =: \mathcal{M}_1$ and $\mathcal{B} =: \mathcal{B}_1$ such that $(\mathcal{M}_1, \mathcal{B}_1, \mathcal{P}_1, \ell_1)$ has Property $\mathfrak{H}$. Now we restrict to all such pairs (i_{11}, i_{13}) satisfying $|\mathcal{M}_1| \le \ell_1$ and $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. We check that $|\mathcal{M}_1| > 2$. Therefore $5 \nmid d$ since $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. Thus there exists i_5 with $0 \le i_5 < 5$ such that $5 \mid n + i_5 d$.

Now we apply Lemma 5 with $p_1 = 5$, $p_2 = 11$ and partition $\mathcal{B}_1(5, 11)$ into two subsets. Let $\mathcal{P}_0 = \Lambda(11, 13) \cup \{11, 13\}$, $(i_1, i_2) = (i_5, i_{11})$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(5, 11) \subseteq \{3, 19, 23\}$ and $\ell \le \ell_2$ where $\ell_2 = 5, 6, 8, 11$ if $k = 13, 17, 19, 23$, respectively. Hence $\mathcal{B}_1'$ is partitioned into $\mathcal{I}_1$ and $\mathcal{I}_2$ satisfying either

$$|\mathcal{I}_1| \le \ell_2, \quad \mathcal{I}_1 \text{ is covered by } \mathcal{P}_2, \quad \mathcal{I}_2 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}_2) \text{ is even}\},$$

or

$$|\mathcal{I}_2| \le \ell_2, \quad \mathcal{I}_2 \text{ is covered by } \mathcal{P}_2, \quad \mathcal{I}_1 = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}_2) \text{ is even}\}.$$

We compute $\mathcal{I}_1, \mathcal{I}_2$ and we restrict attention to those pairs (i_{11}, i_{13}) for which

$\min(|\mathcal{I}_1|,|\mathcal{I}_2|) \le \ell_2$ and either $\mathcal{I}_1$ or $\mathcal{I}_2$ is covered by $\mathcal{P}_2$. We find that $(i_{11}, i_{13}) = (4,2),(5,3)$ if $k = 13$; $(0,0),(5,3)$ if $k = 17$; $(0,0),(0,9),(7,5),(7,9),(8,6),(9,7),(10,8)$ if $k = 19$; and $(0,0),(0,9),(1,10),(2,11),(4,0),(5,1),(5,7),(6,2),(6,8),(7,9),(8,10),(9,11)$ if $k = 23$.

Let (i_{11}, i_{13}) be such a pair. We write M for the one of $\mathcal{I}_1$ or $\mathcal{I}_2$ which is covered by $\mathcal{P}_2$ and B for the other. For $i \in \mathcal{B}'_1$, we see that $p \nmid a_i$ whenever $p \in \mathcal{P}_0$ since $17 \mid a_i$ implies $5 \mid a_i$. Therefore

(18) $\quad \mathfrak{i}(\mathcal{P}_2)$ is even for $i \in B$ and $p \nmid a_i$ for $i \in B$ whenever $p \in \mathcal{P}_0$,

since $B \subseteq \mathcal{B}'_1$. Further we check that $|M| > 1$ if $k \ne 23$ and > 3 if $k = 23$, implying $3 \nmid d$.

By taking $\mathcal{J} = B$, we get $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^+ \cup \mathcal{I}_3^-$ and $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$. Then $p \in \{2,7\}$ whenever $p \mid a_i$ with $i \in \mathcal{I}_3^+ \cup \mathcal{I}_3^-$ by (18). By computing $\mathcal{I}_3^+, \mathcal{I}_3^-$, we find that i's have the same parity in exactly one of $\mathcal{I}_3^+, \mathcal{I}_3^-$. Therefore we deduce from (17) that

$$(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (\{1\},\{7\},\{14\},\{2\}) \text{ or } (\{7\},\{1\},\{2\},\{14\}).$$

Let $k = 13$ and $(i_{11}, i_{13}) = (4,2)$. Then we have $\mathcal{M}_1 = \{0,5,10\}$, $i_5 = 0$, $M = \{3,9,12\}$ and $B = \{1,6,7,8,11\}$ since the latter set is not covered by $\mathcal{P}_2 = \{3\}$. Further $i_3 = 0$, $\mathcal{I}_3^0 = \{6\}$, $\mathcal{I}_3^1 = \mathcal{I}_3^- = \{8,11\}$, $\mathcal{I}_3^2 = \mathcal{I}_3^+ = \{1,7\}$, $\mathcal{I}_5^+ = \{1,6,11\}$, $\mathcal{I}_5^- = \{7,8\}$, $\mathcal{J}_1 = \{11\}$, $\mathcal{J}_2 = \{8\}$, $\mathcal{J}_3 = \{1\}$, $\mathcal{J}_4 = \{7\}$. Hence $a_{11} = 1$, $a_8 = 7$, $a_1 = 14$, $a_7 = 2$ or $a_{11} = 7$, $a_8 = 1$, $a_1 = 2$, $a_7 = 14$. The second possibility is excluded since $a_{11} = 7$, $a_7 = 14$ is not possible. Further, from (18) we get $a_6 = 1$ since $2 \nmid a_6$ and $7 \nmid a_6$. Since $13 \mid n + 2d$ and $7 \mid n + d$, we get $\left(\frac{i-2}{13}\right) = \left(\frac{a_i a_6}{13}\right) = \left(\frac{a_i}{13}\right)$ and $-\left(\frac{i-1}{7}\right) = \left(\frac{a_i a_6}{7}\right) = \left(\frac{a_i}{7}\right)$. We observe that $13 \mid n + 2d$, $11 \mid n + 4d$, $7 \mid n + d$, $5 \mid n$, $3 \mid n$, $2 \mid n + d$, $5 \mid a_i$ for $i \in \mathcal{M}$ and $3 \mid a_i$ for $i \in \mathcal{M}_1$. Now we see that $a_0 \in \{5,15\}$ and $a_0 = 5$ is excluded since $\left(\frac{5}{7}\right) \ne -\left(\frac{-1}{7}\right)$. Thus $a_0 = 15$. Next $a_1 = 14$, $a_2 = 13$ and $a_3 = 3$. Also $a_4 \in \{1,11\}$ and $a_4 \ne 1$ since $\left(\frac{a_4}{13}\right) = \left(\frac{2}{13}\right) = -1$. Similarly we derive that $a_5 = 10$, $a_6 = 1$, $a_7 = 2$, $a_8 = 7$, $a_9 = 6$, $a_{10} = 5$, $a_{11} = 1$ and $a_{12} = 3$. Thus $(a_0, a_1, \ldots, a_{12}) = (15, 14, \ldots, 6, 5, 1, 3)$. The other case $(i_{11}, i_{13}) = (5,3)$ is similar and we get $(a_0, a_1, \ldots, a_{12}) = (1, 15, 14, \ldots, 5, 1)$.

Let $k = 17$ and $(i_{11}, i_{13}) = (0,0)$. Then we have $\mathcal{M}_1 = \{5,10,15\}$ and $i_5 = 0$. We see from the assumption of Lemma 6 with $k = 17$, $k' = 13$ that $4 \le i_{17} < 13$. Hence, from $i_{17} \in \bigcup_{p=5,11,13}\{i_p + pj : 0 \le j < \lceil k/p \rceil\}$, we get $i_{17} \in \{5,10,11\}$. Further $M = \{3,6,12\}$, $B = \{1,2,4,7,8,9,14,16\}$, $i_3 = 0$, $\mathcal{I}_3^0 = \{9\}$, $\mathcal{I}_3^1 = \{1,4,7,16\}$, $\mathcal{I}_3^2 = \{2,8,14\}$, $\mathcal{I}_5^+ = \{1,4,9,14,16\}$, $\mathcal{I}_5^- = \{2,7,8\}$, $\mathcal{J}_1 = \{1,4,16\}$, $\mathcal{J}_2 = \{7\}$, $\mathcal{J}_3 = \{14\}$ and $\mathcal{J}_4 = \{2,8\}$. Therefore $a_1 = a_4 = a_{16} = 1$, $a_7 = 7$, $a_{14} = 14$, $a_2 = a_8 = 2$. Thus $a_9 = 1$ by (18) and $2 \nmid a_9$, $7 \nmid a_9$. Now we see by the Legendre symbol mod 17 that $a_1 = a_4 = a_9 = a_{16} = 1$ is not possible. The case $(i_{11}, i_{13}) = (5,3)$ is excluded similarly.

Let $k = 19$ and $(i_{11}, i_{13}) = (0, 0)$. Then we have $\mathcal{M}_1 = \{5, 10, 15, 17\}$, $i_5 = 0$, $i_{17} = 0$, $M = \{3, 6, 12\}$, $B = \{1, 2, 4, 7, 8, 9, 14, 16, 18\}$ and $i_3 = 0$. We see from $i_{19} \in \bigcup_{p=3,5,11,13,17}\{i_p + pj : 0 \le j < \lceil k/p \rceil\}$ and $2 \le i_{19} < 17$ that $i_{19} \in \{3, 5, 6, 9, 10, 11, 12, 13, 15\}$. Further, $\mathcal{I}_3^0 = \{9, 18\}$, $\mathcal{I}_3^1 = \{1, 4, 7, 16\}$, $\mathcal{I}_3^2 = \{2, 8, 14\}$, $\mathcal{I}_5^+ = \{1, 4, 9, 14, 16\}$, $\mathcal{I}_5^- = \{2, 7, 8, 18\}$, $\mathcal{J}_1 = \{1, 4, 16\}$, $\mathcal{J}_2 = \{7\}$, $\mathcal{J}_3 = \{14\}$ and $\mathcal{J}_4 = \{2, 8\}$. Therefore $a_1 = a_4 = a_{16} = 1$, which is not possible by mod 19. The case $(i_{11}, i_{13}) = (7, 5)$ is excluded similarly. Let $(i_{11}, i_{13}) = (0, 9)$. Then $\mathcal{M}_1 = \{2, 5, 7, 12, 17\}$, $i_5 = 2$, $i_{17} = 5$, $M = \{1, 3, 10, 16\}$, $B = \{4, 6, 8, 13, 14, 15, 18\}$, $i_3 = 1$ and $i_{19} = 3$. We now consider $(n + 6d)(n + 7d) \cdots (n + 18d) = b'y'^2$. Then $P(b') \le 13$. By the case $k = 13$, we get $(a_6, a_7, \ldots, a_{18}) = (1, 15, 14, \ldots, 6, 5, 1)$ since $5 \mid a_7$ and $3 \mid a_{16}$. From $19 \mid n + 3d$, we get $\left(\frac{a_i}{19}\right) = \left(\frac{a_i a_6}{19}\right) = -\left(\frac{i-3}{19}\right)$ which together with $13 \mid n + 9d$, $11 \mid n$, $7 \mid n + d$, $2 \mid n$, $5 \mid a_2$, $17 \mid a_5$, $3 \mid a_1$ implies $a_0 \in \{2, 22\}$, $a_1 \in \{3, 21\}$, $a_2 = 5$, $a_3 = 19$, $a_4 = 2$ and $a_5 = 17$. Now from $\left(\frac{a_i}{17}\right) = \left(\frac{a_i a_6}{17}\right) = \left(\frac{i-5}{17}\right)$, we get $a_0 = 22$, $a_1 = 21$. Thus $(a_0, a_1, \ldots, a_{18}) = (22, 21, \ldots, 6, 5, 1)$. The case $(i_{11}, i_{13}) = (7, 9)$ is similar and we get $(a_0, a_1, \ldots, a_{18}) = (1, 5, 6, \ldots, 21, 22)$. For the pair $(i_{11}, i_{13}) = (10, 8)$, we similarly get $(a_0, a_1, \ldots, a_{18}) = (21, 5, \ldots, 6, 5, 1, 3)$. This is excluded by considering $(n + 3d)(n + 6d) \cdots (n + 18d)$ and $k = 6$. For the pairs $(i_{11}, i_{13}) = (8, 6), (9, 7)$, we get $i_{19} = 0, 1$, respectively, which is not possible since $i_{19} \ge 2$ by the assumption of the lemma.

Let $k = 23$ and $(i_{11}, i_{13}) = (0, 0)$. Then $\mathcal{M}_1 = \{5, 10, 15, 17, 20\}$, $i_5 = 0$, $i_{17} = 0$, $M = \{3, 6, 12, 19, 21\}$, $B = \{1, 2, 4, 7, 8, 9, 14, 16, 18\}$, $i_3 = 0$ and $i_{19} = 0$ since $23 \nmid a_{19}$. We have $i_{23} \in \{5, 6, 9, 10, 11, 12, 13, 15, 17, 18\}$ since $4 \le i_{23} < 19$. Here we observe that $23 \nmid a_{19}$ and $4 \le i_{23} < 19$ in view of our assumption that $k \nmid a_i$ for $0 \le i < k - k'$ and $k' \le i < k$ with $k = 23$, $k' = 19$. Further, $\mathcal{I}_3^0 = \{9, 18\}$, $\mathcal{I}_3^1 = \{1, 4, 7, 16\}$, $\mathcal{I}_3^2 = \{2, 8, 14\}$, $\mathcal{I}_5^+ = \{1, 4, 9, 14, 16\}$, $\mathcal{I}_5^- = \{2, 7, 8, 18\}$, $\mathcal{J}_1 = \{1, 4, 16\}$, $\mathcal{J}_2 = \{7\}$, $\mathcal{J}_3 = \{14\}$ and $\mathcal{J}_4 = \{2, 8\}$. Therefore $a_1 = a_4 = a_{16} = 1$, $a_7 = 7$, $a_{14} = 14$, $a_2 = a_8 = 2$. This is not possible since $\left(\frac{a_1}{23}\right) = \left(\frac{a_4}{23}\right) = \left(\frac{a_{16}}{23}\right) = \left(\frac{a_2}{23}\right) = \left(\frac{a_8}{23}\right) = 1$. The cases $(i_{11}, i_{13}) = (0, 9), (1, 10), (2, 11), (4, 0), (7, 9), (8, 10), (9, 11)$ are excluded similarly. Let $(i_{11}, i_{13}) = (5, 1)$. Then $\mathcal{M}_1 = \{7, 10, 12, 17, 22\}$, $i_5 = 2$, $i_{17} = 10$, $M = \{0, 3, 4, 6, 8, 15, 21\}$, $B = \{9, 11, 13, 18, 19, 20\}$ and $i_3 = 0$. This implies either $23 \mid a_4$, $19 \mid a_8$ or $23 \mid a_8$, $19 \mid a_4$. Further, $\mathcal{I}_3^0 = \{9, 18\}$, $\mathcal{I}_3^1 = \{11, 20\}$, $\mathcal{I}_3^2 = \{13, 19\}$, $\mathcal{I}_5^+ = \{11, 13, 18\}$, $\mathcal{I}_5^- = \{9, 19, 20\}$, $\mathcal{J}_1 = \{11\}$, $\mathcal{J}_2 = \{20\}$, $\mathcal{J}_3 = \{13\}$ and $\mathcal{J}_4 = \{19\}$. Therefore $a_{11} = 1$, $a_{20} = 7$, $a_{13} = 14$, $a_{19} = 2$. Further, from (18) we get $a_9 \in \{1, 2\}$, $a_{18} = 1$ since $7 \nmid a_9 a_{18}$, $2 \nmid a_{18}$. However, $a_9 = 2$ as $9 \in \mathcal{I}_5^-$, $18 \in \mathcal{I}_5^+$. Since $\left(\frac{a_{11}}{23}\right) = \left(\frac{a_{18}}{23}\right) = 1$, we see that $23 \mid a_4$, $19 \mid a_8$. By using $\left(\frac{a_i}{p}\right) = \left(\frac{a_i a_{11}}{p}\right) = \left(\frac{(i - i_p)(11 - i_p)}{p}\right)$, we get $\left(\frac{a_i}{23}\right) = -\left(\frac{i-4}{23}\right)$, $\left(\frac{a_i}{11}\right) = -\left(\frac{i-5}{11}\right)$, $\left(\frac{a_i}{7}\right) = -\left(\frac{i-6}{7}\right)$ and $\left(\frac{a_i}{5}\right) = \left(\frac{i-2}{5}\right)$. Now from $23 \mid a_4$, $19 \mid a_8$, $17 \mid a_{10}$, $13 \mid n + d$, $11 \mid n + 5d$, $7 \mid n + 6d$, $5 \mid n + 2d$, $3 \mid n$, $2 \mid n + d$, $\mathcal{M}_1$ being covered by $\{5, 17\}$, and M by $\{3, 19, 23\}$, we derive that $(a_0, a_1, \dots, a_{22}) = (3, 26, \dots, 6, 5)$. The cases $(i_{11}, i_{13}) = (5, 7), (6, 2), (6, 8)$ are similar and we get $(a_0, a_1, \dots, a_{22}) = (6, 7, \dots, 3, 7), (7, 3, \dots, 7, 6), (5, 6, 7, \dots, 3)$, respectively.

3.4. *Introductory remarks on the cases* $k \geq 29$. Assume $q_1 \nmid d$ and $q_2 \nmid d$. Then, by taking the mirror image (4) of (2), there is no loss of generality in assuming that $q_1 \mid n + i_{q_1} d$, $q_2 \mid n + i_{q_2} d$ for some pair (i_{q_1}, i_{q_2}) with $0 \leq i_{q_1} < q_1$, $0 \leq i_{q_2} \leq (k-1)/2$ and further $i_{q_2} \geq k - k'$ if $q_2 = k$. For $k = 61$, by taking $(n + 8d) \cdots (n + 60d)$ and $k = 53$, we may assume that $\max(i_{59}, i_{61}) \geq 8$ if $i_{59} \geq 2$. Let $\mathcal{P}_0 = \emptyset$, $p_1 = q_1$, $p_2 = q_2$, $(i_1, i_2) = (i_{q_1}, i_{q_2})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \mathcal{P}_1 := \Lambda(q_1, q_2)$ and $\ell \leq \ell_1 = \sum_{p \in \mathcal{P}_1} \lceil k/p \rceil$. We check that $\ell_1 < \frac{1}{2}|\mathcal{I}'|$ since $|\mathcal{I}'| \geq k - \lceil k/q_1 \rceil - \lceil k/q_2 \rceil$. By Corollary 1, we get $\mathcal{M} =: \mathcal{M}_1$ and $\mathcal{B} =: \mathcal{B}_1$ with $(\mathcal{M}_1, \mathcal{B}_1, \mathcal{P}_1, \ell_1)$ having Property $\mathfrak{H}$. We now restrict to all such pairs (i_{q_1}, i_{q_2}) for which $|\mathcal{M}_1| \leq \ell_1$ and $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. We find that there is no such pair (i_{q_1}, i_{q_2}) when $k = 97$.

3.5. *The cases* $29 \leq k \leq 59$. As stated in Lemma 6, we have $q_1 = 19$, $q_2 = 29$ and $\mathcal{P}_1 = \Lambda(19, 29) \subseteq \{11, 13, 17, 43, 47, 53, 59\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by

$$\begin{aligned}
k = 29 &: (0,9), (1,10), (2,11), (3,12), (4,13), (15,5), (16,6), (17,7), (18,8);\\
k = 31 &: (0,0), (0,9), (1,10), (2,11), (3,12), (4,13), (11,1),\\
&\quad (12,2), (13,3), (14,4), (15,5), (16,6), (17,7), (18,8);\\
k = 37 &: (0,0), (0,9), (1,10), (2,11), (3,12), (4,13), (17,7), (18,8);\\
k = 41 &: (0,0), (2,11), (3,12), (4,13);\\
k = 43 &: (0,0), (1,1), (3,12), (4,13), (5,14), (6,15), (7,16), (8,17);\\
k = 47 &: (0,0), (1,1), (7,16), (8,17), (9,18), (10,19), (11,20),\\
&\quad (12,21), (13,22), (13,23), (14,23);\\
k = 53 &: (0,0), (1,0), (1,1), (13,22), (13,23), (14,23), (14,24),\\
&\quad (15,24), (15,25), (16,25), (16,26), (17,26);\\
k = 59 &: (0,0), (0,28), (1,0), (1,1), (2,1), (3,2), (17,27), (18,28).
\end{aligned}$$

Let $k = 31$ and $(i_{19}, i_{29}) = (0, 9)$. We see that $\mathcal{P}_1 = \{11, 13, 17\}$, $\mathcal{M}_1 = \{4, 5, 12, 16, 21, 25, 27\}$ and $\mathcal{B}_1 = \{1, 2, 3, 6, 7, 8, 10, 11, 13, 14, 15, 17, 18, 20, 22, 23, 24, 26, 28, 29, 30\}$. Since $\mathcal{M}_1$ is covered by $\mathcal{P}_1$, we find that 11 divides a_5, a_{16}, a_{27}; 13 divides a_{12}, a_{25}; and 17 divides a_4, a_{21}. Hence $i_{11} = 5$, $i_{13} = 12$, $i_{17} = 4$. We see that $\gcd(11 \cdot 13 \cdot 17, a_i) = 1$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{19, 29\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (i_{11}, i_{13}) = (5, 12)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31\}$ and $\ell \leq \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 8$. Thus $|\mathcal{I}'| = |\mathcal{B}_1| = 21 > 2\ell_2$. Then the conditions of Corollary 1 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$. We get $\mathcal{M}_2 = \{1, 3, 7, 8, 18, 23, 28\}$. This is not possible since $\mathcal{M}_2$ is not covered by $\mathcal{P}_2$. Further, the following pairs (i_{19}, i_{29}) are excluded similarly:

$$k = 29 : (0,9), (1,10), (2,11), (3,12), (4,13), (15,5), (16,6), (17,7), (18,8);$$
$$k = 31 : (1,10), (2,11), (3,12), (4,13), (18,8).$$

Thus $k > 29$.

Let $k = 59$ and $(i_{19}, i_{29}) = (0,0)$. Then we see that $\mathcal{P}_1 = \{11, 13, 17, 43, 47, 53, 59\}$, $\mathcal{M}_1 = \{11, 13, 17, 22, 26, 33, 34, 39, 43, 44, 47, 51, 52, 53, 55\}$, $\mathcal{B}_1 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 23, 24, 25, 27, 28, 30, 31, 32, 35, 36, 37, 40, 41, 42, 45, 46, 48, 49, 50, 54, 56\}$, $i_{11} = i_{13} = i_{17} = 0$, $\{43, 47, 53\}$ is covered by $\{43, 47, 53, 59\} =: \mathcal{P}_1'$. Let $p \mid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. Then we show that $i \in \{4, 6, 10\}$. Let $59 \mid a_{43}$. Then $\{47, 53\}$ is covered by $\{43, 47, 53\}$. Let $43 \mid a_{47}$. If $43 \mid a_i$ with $i \in \mathcal{B}_1$, then $i = 4$ and $43p \mid a_4$ with $p \in \{47, 53\}$ since $\mathfrak{i}(\mathcal{P}_1)$ is even. This implies either $53 \mid a_{53}, 43 \cdot 47 \mid a_4$ or $47 \mid a_{53}, 43 \cdot 53 \mid a_4$. Similarly we get $i \in \{4, 6, 10\}$ by considering all the cases $59 \mid a_{43}$, $59 \mid a_{47}$ and $59 \nmid a_{43}a_{47}a_{53}$. We observe that $59 \nmid a_{53}$ since $6 \le i_{59} < 53$. Hence we conclude that $p \nmid a_i$ for $i \in \mathcal{B}_1 \setminus \{4, 6, 10\}$ and $p \in \mathcal{P}_1'$. Further we observe that

$$i_{59} \in \mathcal{M}_1 \cup \{19, 29, 38\} \cup \{6, 10\}. \tag{19}$$

Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{19, 29\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (0, 0)$, $\mathcal{I} = \mathcal{B}_1 \setminus \{4, 6, 10\}$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31, 37\}$ and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 16$. Thus $|\mathcal{I}'| = |\mathcal{B}_1| - 2 > 2\ell_2$. Then the conditions of Corollary 1 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ with $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ having Property $\mathfrak{H}$. We get $\mathcal{M}_2 = \{5, 15, 20, 30, 31, 35, 37, 40, 45\}$, $\mathcal{B}_2 = \{1, 2, 3, 7, 8, 9, 12, 14, 16, 18, 21, 23, 24, 25, 27, 28, 32, 36, 41, 42, 46, 48, 49, 50, 54, 56\}$, $i_5 = 0$, and $31 \mid a_{31}$, $37 \mid a_{37}$ or $31 \mid a_{37}$, $37 \mid a_{31}$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{19, 29\}$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) := (0, 0)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 23, 41\}$ and $\ell \le \ell_3 = \sum_{p \in \mathcal{P}_3} \lceil k/p \rceil$. Then by Lemma 5, we see that $M = \{3, 6, 12, 21, 23, 24, 27, 41, 42, 46, 48, 54\}$ is covered by $\mathcal{P}_3$ and $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B = \{1, 2, 7, 8, 9, 14, 16, 18, 28, 32, 36, 49, 56\}$. Thus $i_3 = i_{23} = i_{41} = 0$ and $p \in \{2, 7\}$ whenever $p \mid a_i$ with $i \in B$. Putting $\mathcal{J} = B$, we have $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^2$ and $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

$$\mathcal{I}_3^0 = \{9, 18, 36\}, \quad \mathcal{I}_3^1 = \{1, 7, 16, 28, 49\}, \quad \mathcal{I}_3^2 = \{2, 8, 14, 32, 56\}$$

and

$$\mathcal{I}_5^+ = \{1, 9, 14, 16, 36, 49, 56\}, \quad \mathcal{I}_5^- = \{2, 7, 8, 18, 28, 32\},$$

so that

$$\mathcal{J}_1 = \{1, 16, 49\}, \quad \mathcal{J}_2 = \{7, 28\}, \quad \mathcal{J}_3 = \{14, 56\}, \quad \mathcal{J}_4 = \{2, 8, 32\}.$$

Hence $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (\{1\}, \{7\}, \{14\}, \{2\})$ by (17). Thus $a_1 = a_{16} = a_{49} = 1$, $a_7 = a_{28} = 7$, $a_{14} = a_{56} = 14$, $a_2 = a_8 = a_{32} = 2$. Further, we get

$a_9 = a_{36} = 1$ and $a_{18} = 2$ since $9, 36 \in \mathcal{I}_5^+$ and $18 \in \mathcal{I}_5^-$. Since

$$\left(\frac{a_i}{59}\right) = 1 \quad \text{for } a_i \in \{1, 7\}, \tag{20}$$

we see that $\left(\frac{a_i}{59}\right) = 1$ for $i \in \{1, 7, 9, 16, 28, 36, 49\}$, which is not possible by (19).

Let $k = 41$ and $(i_{19}, i_{29}) = (2, 11)$. Then we see that $\mathcal{P}_1 = \{11, 13, 17\}$, $\mathcal{M}_1 = \{1, 6, 7, 14, 18, 23, 27, 29\}$, $\mathcal{B}_1 = \{0, 3, 4, 5, 8, 9, 10, 12, 13, 15, 16, 17, 19, 20, 22, 24, 25, 26, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39\}$, $i_{11} = 7$, $i_{13} = 1$, $i_{17} = 6$. Further $\gcd(a_i, 11 \cdot 13 \cdot 17) = 1$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{19, 29\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (7, 1)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31, 37\}$ and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 13$. Then $|\mathcal{I}'| = |\mathcal{B}_1| > 2\ell_2$. Thus the conditions of Corollary 1 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$ and $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$. We have $\mathcal{M}_2 = \{0, 3, 5, 9, 10, 20, 25, 30, 35\}$, $\mathcal{B}_2 = \{4, 8, 12, 13, 15, 16, 17, 19, 22, 24, 26, 28, 31, 32, 33, 34, 36, 37, 38, 39\}$, $i_5 = 0$. Further $31 \cdot 37 \mid a_3 a_9$, $31 \nmid a_{34}$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{19, 29\}$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) := (0, 7)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 23, 41\}$, $\ell \le \sum_{p \in \mathcal{P}_3} \lceil k/p \rceil$ and apply Lemma 5 to see that $M = \{13, 16, 17, 19, 28, 34, 37\}$ is covered by $\mathcal{P}_3$, $i_3 = 1$, $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B = \{4, 8, 12, 22, 24, 26, 31, 32, 33, 36, 38, 39\}$. Further, $i_{23} = 17$, $i_{41} \in \{2, 11, 21\} \cup \mathcal{M}_1 \cup \mathcal{M}_2 \cup M \cup \{4, 22, 31\}$ or *vice versa*. Here we observe that i_{41} exists since $41 \nmid d$. Thus $23 \cdot 41 \mid \prod a_i$ where i runs through the set $\{2, 11, 21\} \cup \mathcal{M}_1 \cup \mathcal{M}_2 \cup \{4, 22, 31\}$. Therefore $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{I}_3^1 \cup \mathcal{I}_3^2$, where $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^2$, $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

$$\mathcal{I}_3^0 = \{4, 22, 31\}, \quad \mathcal{I}_3^1 = \{12, 24, 33, 36, 39\}, \quad \mathcal{I}_3^2 = \{8, 26, 32, 38\}$$

and

$$\mathcal{I}_5^+ = \{4, 24, 26, 31, 36, 39\}, \quad \mathcal{I}_5^- = \{8, 12, 22, 32, 33, 38\}$$

by taking $\mathcal{J} = B$. We get

$$\mathcal{J}_1 = \{24, 36, 39\}, \quad \mathcal{J}_2 = \{12, 33\}, \quad \mathcal{J}_3 = \{26\}, \quad \mathcal{J}_4 = \{8, 32, 38\},$$

and $a_{24} = a_{36} = a_{39} = 1, a_{12} = a_{33} = 7, a_{26} = 14, a_8 = a_{32} = a_{38} = 2$ by (17). Since

$$\left(\frac{a_i}{41}\right) = 1 \quad \text{for } a_i \in \{1, 2\}, \tag{21}$$

we see that $\left(\frac{a_i}{41}\right) = 1$ for $i \in \{8, 24, 32, 36, 38, 39\}$, which is not valid by the possibilities for i_{41}.

All other cases are excluded similarly. Analogously to (20) and (21), we use $\left(\frac{a_i}{k}\right) = 1$ for

$$a_i \in \begin{cases} \{1,7\} & \text{if } k = 37, 53, 59, \\ \{1,2\} & \text{if } k = 31, 41, 47, \\ \{1,14\} & \text{if } k = 43 \end{cases}$$

to exclude the remaining possibilities.

3.6. *The case* $k = 61$. We have $q_1 = 59$, $q_2 = 61$ and $\mathcal{P}_1 = \{7, 13, 17, 29, 47, 53\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by $(8,6), (9,7), (10,8), (11,9)$, i.e. $(i+2, i)$ with $6 \le i \le 9$.

Let $(i_{59}, i_{61}) = (8,6)$. Then $\mathcal{P}_1 = \{7, 13, 17, 29, 47, 53\}$, $\mathcal{M}_1 = \{2, 4, 9, 11, 14, 15, 16, 20, 25, 28, 32, 33, 38, 39, 41, 46, 50, 53, 54, 60\}$, $\mathcal{B}_1 = \{0, 1, 3, 5, 7, 10, 12, 13, 17, 18, 19, 21, 22, 23, 24, 26, 27, 29, 30, 31, 34, 35, 36, 37, 40, 42, 43, 44, 45, 47, 48, 49, 51, 52, 55, 56, 57, 58, 59\}$, $i_7 = 4$, $i_{13} = 2$, $i_{17} = 16$, $i_{29} = 9$ and a_{14}, a_{20} are divisible by $47, 53$. Further, $\gcd(p, a_i) = 1$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. Let $\mathcal{P}_0 = \mathcal{P}_1 \cup \{59, 61\}$, $p_1 = 7$, $p_2 = 17$, $(i_1, i_2) := (4, 16)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(7, 17) \setminus \mathcal{P}_0 = \{11, 19, 23, 37\}$ and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 15$. Then $2\ell_2 < |\mathcal{I}'| = |\mathcal{B}_1| - 1$. By Corollary 1, we get $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$. We find that $\mathcal{M}_2 = \{1, 10, 12, 21, 23, 29, 30, 34, 44, 45, 48, 56\}$, $\mathcal{B}_2 = \{0, 3, 5, 7, 13, 17, 19, 22, 24, 26, 27, 31, 35, 36, 37, 40, 42, 43, 47, 49, 51, 52, 55, 57, 58, 59\}$, $i_{11} = 1$, $i_{19} = 10$, $i_{23} = 21$, $i_{37} = 30$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{59, 61\}$, $p_1 = 11$, $p_2 = 59$, $(i_1, i_2) := (1, 8)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 59) \setminus \mathcal{P}_0 = \{31, 41\}$ and $\ell \le \ell_3 = \sum_{p \in \mathcal{P}_3} \lceil k/p \rceil = 4$. Then $2\ell_3 < |\mathcal{I}'| = |\mathcal{B}_2|$. By Corollary 1, we get $\mathcal{M} =: \mathcal{M}_3$ and $\mathcal{B} =: \mathcal{B}_3$ such that $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ has Property $\mathfrak{H}$. We get $\mathcal{M}_3 = \{0, 5, 26, 36\}$, which cannot be covered by $\mathcal{P}_3$. This is a contradiction. The remaining cases are excluded similarly.

3.7. *The cases* $k = 67, 71$. We have $q_1 = 43$, $q_2 = 67$ and $\mathcal{P}_1 \subseteq \{11, 13, 19, 29, 31, 37, 41, 53, 71\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by

$k = 67 : (i, i)$, $6 \le i \le 33$;

$k = 71 : (i, i)$, $0 \le i \le 35$, $i \ne 24, 25$, and $(24, 0), (25, 1), (26, 2), (27, 3)$.

Let $k = 71$ and $(i_{43}, i_{67}) = (27, 3)$. We see that $\mathcal{P}_1 = \{11, 13, 19, 29, 31, 37, 41, 53, 71\}$, $\mathcal{M}_1 = \{4, 5, 8, 12, 13, 15, 17, 18, 26, 29, 31, 32, 33, 37, 39, 41, 44, 48, 51, 57, 59\}$, $\mathcal{B}_1 = \{0, 1, 2, 6, 7, 9, 10, 11, 14, 16, 19, 20, 21, 22, 23, 24, 25, 28, 30, 34, 35, 36, 38, 40, 42, 43, 45, 46, 47, 49, 50, 52, 53, 54, 55, 56, 58, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69\}$, $i_{11} = 4$, $i_{13} = 5$, $i_{19} = 13$. Therefore $\{8, 12, 17, 29, 33, 39, 41\}$ is covered by $\{29, 31, 37, 41, 53, 71\}$ implying either $i_{29} = 12$ or $i_{29} \in \{17, 29, 33\}$, $i_{31} = 8$. Let $i \in \mathcal{B}_1$ and $p \mid a_i$ with $p \in \mathcal{P}_1$. Then there is a $q \in \mathcal{P}_1$ such that $pq \mid a_i$ since $\mathfrak{i}(\mathcal{P}_1)$ is even. Next we consider the case $i_{31} = 8$. Then $\{12, 17, 29, 33, 41\} =: \mathcal{M}_1'$ is covered by $\{29, 37, 41, 53, 71\}$ and $i_{29} \ne 12$. For $29 \in \mathcal{M}_1'$, we may suppose that either $29 \mid a_{29}$, $41 \mid a_{17}$, $29 \cdot 41 \mid a_{58}$ or $29 \mid a_{29}$, $41 \mid a_{41}$, $29 \cdot 41 \mid a_0$. Thus 0 or 58 in $\mathcal{B}_1$ correspond to 29. We argue as above that for any other element of $\mathcal{M}_1'$, there is no corresponding element in $\mathcal{B}_1$.

For the first case, we derive similarly that $31\,|\,a_{33}$, $37\,|\,a_{39}$, $31\cdot 37\,|\,a_2$ or $37\,|\,a_{17}$, $37\cdot 71\,|\,a_{54}$ or $37\,|\,a_{29}$, $37\cdot 71\,|\,a_{63}$ or $41\,|\,a_{17}$, $37\cdot 71\,|\,a_{58}$. Therefore

$$29\cdot 31\cdot 37\cdot 41\cdot 53\cdot 71 \,\Big|\, \prod (n+id) \quad \text{for } i\in \mathcal{M}_1\cup\{3,27,70\}\cup\mathcal{B}_1'$$

where $\mathcal{B}_1'=\{2,54,58,63\}$ if $i_{29}=12$ and $\{0,58\}$ otherwise. Further,

$$i_{71}\in\mathcal{M}_1\cup\{27\}\cup\mathcal{B}_1' \quad\text{and}\quad i_{71}\neq 32. \tag{22}$$

For each possibility $i_{29}\in\{0,4,12,17\}$, we now take $\mathcal{P}_0=\mathcal{P}_1\cup\{43,67\}$, $p_1=19, p_2=29$, $(i_1,i_2):=(13,i_{29})$, $\mathcal{I}=\mathcal{B}_1\backslash\mathcal{B}_1'$, $\mathcal{P}=\mathcal{P}_2:=\Lambda(19,29)\backslash\mathcal{P}_0=\{17,47,59,61\}$ and $\ell=\ell_2=\sum_{p\in\mathcal{P}_2}\lceil k/p\rceil=11$. Then $|\mathcal{I}'|=|\mathcal{B}_1|-4>2\ell_2$. Thus the conditions of Corollary 1 are satisfied and we get $\mathcal{M}=:\mathcal{M}_2$ and $\mathcal{B}=:\mathcal{B}_2$ with $(\mathcal{M}_2,\mathcal{B}_2,\mathcal{P}_2,\ell_2)$ having Property $\mathfrak{H}$. We check that $|\mathcal{M}_2|\le\ell_2$ only at $i_{29}=12$, in which case we get $\mathcal{M}_2=\{9,11,19,23,36,53\}$, $\mathcal{B}_2=\{0, 1, 6, 7, 10, 14, 16, 20, 21, 22, 24, 25, 28, 30, 34, 35, 38, 40, 42, 43, 45, 46, 47, 49, 50, 52, 55, 56, 60, 61, 62, 63, 64, 65, 67, 68, 69\}$, $i_{17}=2$ and $\{9,11,23\}$ is covered by $\{47,59,61\}$. Thus $47\cdot 59\cdot 61\mid a_9a_{11}a_{23}$. Further, $p\nmid a_i$ for $i\in\mathcal{B}_2$ and $p\in\mathcal{P}_2$. We now take $\mathcal{P}_0=\mathcal{P}_1\cup\mathcal{P}_2\cup\{43,67\}$, $p_1=11$, $p_2=13$, $(i_1,i_2):=(4,5)$, $\mathcal{I}=\mathcal{B}_2$, $\mathcal{P}=\mathcal{P}_3:=\Lambda(11,13)\backslash\mathcal{P}_0=\{5\}$ and $\ell=\ell_3=\lceil k/5\rceil=15$. Then $|\mathcal{I}'|=|\mathcal{B}_2|>2\ell_3$. By Corollary 1, we get $\mathcal{M}=:\mathcal{M}_3$ and $\mathcal{B}=:\mathcal{B}_3$ such that $(\mathcal{M}_3,\mathcal{B}_3,\mathcal{P}_3,\ell_3)$ has Property $\mathfrak{H}$. We calculate $\mathcal{M}_3=\{0,10,25,30,35,40,50,55, 60, 65\}$, $\mathcal{B}_3=\{1, 6, 7, 14, 16, 20, 21, 22, 24, 28, 34, 38, 42, 43, 45, 46, 47, 49, 52, 54, 56, 58, 61, 62, 63, 64, 66, 67, 68, 69\}$, $i_5=0$ and further $5\nmid a_{20}a_{45}$. Lastly, we take $\mathcal{P}_0=\mathcal{P}_1\cup\mathcal{P}_2\cup\mathcal{P}_3\cup\{43,67\}$, $p_1=5$, $p_2=11$, $(i_1,i_2):=(0,4)$, $\mathcal{I}=\mathcal{B}_3$, $\mathcal{P}=\mathcal{P}_4:=\Lambda(5,11)\setminus\mathcal{P}_0=\{3,23\}$ and $\ell=\ell_4=\sum_{p\in\mathcal{P}_4}\lceil k/p\rceil$. By Lemma 5, we see that $M=\{16,22,24,28,43,46,47,49,64,67\}$ is covered by $\mathcal{P}_4$, $i_3=i_{23}=1$, $B=\{1,6,7,14,21,34,38,42,52,56,61,62,63,68,69\}$ and hence $3\nmid a_7a_{34}a_{52}a_{61}$ and possibly $3\cdot 23\,|\,a_1$. Therefore $a_i\in\{1,2,7,14\}$ for $i\in B\backslash\{1\}$. By taking $\mathcal{J}=B\backslash\{1\}$, we have $B\backslash\{1\}=\mathcal{I}_3^0\cup\mathcal{I}_3^1\cup\mathcal{I}_3^-=\mathcal{I}_5^+\cup\mathcal{I}_5^-$ with

$$\mathcal{I}_3^0=\{7,34,52,61\},\qquad \mathcal{I}_3^1=\{6,21,42,63,69\},\qquad \mathcal{I}_3^-=\{14,38,56,62,68\}$$

and

$$\mathcal{I}_5^+=\{6,14,21,34,56,61,69\},\qquad \mathcal{I}_5^-=\{7,38,42,52,62,63,68\}.$$

Therefore

$$\mathcal{J}_1=\{6,21,69\},\qquad \mathcal{J}_2=\{42,63\},\qquad \mathcal{J}_3=\{14,56\},\qquad \mathcal{J}_4=\{38,62,68\},$$

and hence $a_6=a_{21}=a_{69}=1$, $a_{42}=a_{63}=7$, $a_{14}=a_{56}=14$, $a_{38}=a_{62}=a_{68}=2$ by (17). Further, we get $a_{34}=a_{61}=1$ and $a_{52}=2$ by taking residue classes modulo 5. Since $\left(\frac{1}{71}\right)=\left(\frac{2}{71}\right)=1$, we see that $\left(\frac{a_i}{71}\right)=1$ for $i\in\{6,21,34,38,52,61,62,68,69\}$, which is not valid by the possibilities for i_{71} given by (22).

Let $k = 67$ and $(i_{43}, i_{67}) = (9, 9)$. We see that $\mathcal{P}_1 = \{11, 13, 19, 29, 31, 37, 41, 53\}$, $\mathcal{M}_1 = \{20, 22, 28, 31, 35, 38, 40, 42, 46, 47, 48, 50, 53, 61, 62, 64, 66\}$, $\mathcal{B}_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 23, 24, 25, 26, 27, 29, 30, 32, 33, 34, 36, 37, 39, 41, 43, 44, 45, 49, 51, 54, 55, 56, 57, 58, 59, 60, 63, 65\}$, $i_{11} = i_{13} = i_{19} = 9$ and $\{38, 40, 46, 50, 62\}$ is covered by $\{29, 31, 37, 41, 53\}$. Further, $p \nmid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$ except possibly when $29 \mid a_{50}$, $41 \mid a_{62}$, $29 \cdot 41 \mid a_{21}$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{43, 67\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (9, 9)$, $\mathcal{I} = \mathcal{B}_1 \setminus \{21\}$ and $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 17, 47, 59, 61\}$. If $5 \nmid d$, we observe that there is at least one multiple of 5 among $n + (i_{11} + 11i)d$, $0 \le i \le 5$, and $\ell \le \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil - 1 = 23$. Thus we always have $\ell \le 23 = \ell_2$. Then $|\mathcal{I}'| = |\mathcal{B}_1| - 1 > 2\ell_2$ since $|B_1| = 48$. Thus the conditions of Corollary 1 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$. We have $\mathcal{M}_2 = \{0, 1, 2, 3, 5, 6, 7, 8, 14, 19, 24, 26, 29, 39, 43, 44, 49, 54, 56, 60\}$, which cannot be covered by $\mathcal{P}_2$. This is a contradiction. The cases $k = 67$, $(i_{43}, i_{67}) = (i, i)$ with $9 \le i \le 28$, and $k = 71$, $(i_{43}, i_{67}) = (i, i)$ with $13 \le i \le 28$, $i \ne 24, 25$, are excluded in the same way as in this paragraph. The remaining cases are excluded in the same way as $k = 71$, $(i_{43}, i_{67}) = (27, 3)$ given in the preceding paragraph.

3.8. *The cases* $k = 73, 79$. We have $q_1 = 23$, $q_2 = 73$ and $\mathcal{P}_1 \subseteq \{13, 19, 29, 31, 37, 47, 59, 61, 67, 79\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by

$$\begin{aligned} k = 73 &: (6,2), (7,3), (8,4), (9,5);\\ k = 79 &: (0,0), (1,1), (2,2), (7,3), (8,4), (9,5), (10,6), (11,7), (12,8),\\ &\quad (13,9), (14,10), (15,11), (16,12), (17,13), (18,14), (19,15). \end{aligned}$$

These pairs are of the form $(i + 4, i)$ except for $(0,0), (1,1), (2,2)$ in the case $k = 79$.

Let $k = 79$ and $(i_{23}, i_{73}) = (8, 4)$. We see that $\mathcal{P}_1 = \{13, 19, 29, 31, 37, 47, 59, 61, 67, 79\}$, $\mathcal{M}_1 = \{1, 3, 10, 12, 15, 16, 18, 19, 20, 25, 30, 38, 39, 40, 46, 48, 51, 58, 64, 78\}$, $\mathcal{B}_1 = \{0, 2, 5, 6, 7, 9, 11, 13, 14, 17, 21, 22, 23, 24, 26, 27, 28, 29, 32, 33, 34, 35, 36, 37, 41, 42, 43, 44, 45, 47, 49, 50, 52, 53, 55, 56, 57, 59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76\}$, $i_{13} = 12$, $i_{19} = 1$ and $\{3, 10, 15, 16, 18, 19, 30, 40, 46, 48, 78\}$ is covered by $\{29, 31, 37, 47, 59, 61, 67, 79\}$. Thus

$$29 \cdot 31 \cdot 37 \cdot 47 \cdot 59 \cdot 61 \cdot 67 \cdot 79 \mid \prod (n + id) \qquad \text{for } i \in \{3, 10, 15, 16, 18, 19, 30, 40, 46, 48, 78\}.$$

Further, we have

$$i_{79} \in \{10, 15, 16, 18, 19, 30, 40, 46, 48\} \tag{23}$$

and either $i_{29} = 19$ or $i_{29} \in \{1, 10, 16, 18\}$, $i_{31} = 15$, $i_{37} = 3$, $i_{59} = 19$. Also, for $p \in \mathcal{P}_1$, we have $p \nmid a_i$ for $i \in \mathcal{B}_1$ since $\mathfrak{i}(\mathcal{P}_1)$ is even for $i \in \mathcal{B}_1$.

For each possibility $i_{29} \in \{1, 10, 16, 18, 19\}$, we now take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{23, 73\}$, $p_1 = 19$, $p_2 = 29$, $(i_1, i_2) := (1, i_{29})$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(19, 29) \setminus \mathcal{P}_0 = \{11, 17, 43, 53, 71\}$ and $\ell = \ell_2 = \sum_{p\in\mathcal{P}_2} \lceil k/p \rceil = 19$. Then $|\mathcal{I}'| \geq |\mathcal{B}_1| - 2 > 2\ell_2$. Thus the conditions of Corollary 1 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$, implying $i_{29} = 19$, in which case we get $\mathcal{M}_2 = \{0, 6, 9, 11, 22, 24, 26, 33, 34, 43, 44, 55, 60, 66\}$, $\mathcal{B}_2 = \{2, 5, 7, 13, 14, 17, 21, 23, 27, 28, 29, 32, 35, 36, 37, 41, 42, 45, 47, 49, 50, 52, 53, 56, 57, 59, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76\}$, $i_{11} = 0$, $i_{17} = 9$ and $\{6, 24, 34\}$ is covered by $\{43, 53, 71\}$. Thus $43 \cdot 53 \cdot 71 \mid a_6 a_{24} a_{34}$. Further, $p \nmid a_i$ for $i \in \mathcal{B}_2$ and $p \in \mathcal{P}_2$. We now take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{23, 73\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (0, 12)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5\}$ and $\ell = \ell_3 = \lceil k/5 \rceil = 16$. Then $|\mathcal{I}'| = |\mathcal{B}_2| > 2\ell_3$. By Corollary 1, we get $\mathcal{M} =: \mathcal{M}_3$ and $\mathcal{B} =: \mathcal{B}_3$ with $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ having Property $\mathfrak{H}$. We calculate $\mathcal{M}_3 = \{7, 17, 32, 37, 42, 47, 57, 62, 67, 72\}$, $\mathcal{B}_3 = \{2, 5, 13, 14, 21, 23, 27, 28, 29, 35, 36, 41, 45, 49, 50, 52, 53, 56, 59, 61, 63, 65, 68, 69, 70, 71, 73, 74, 75, 76\}$, $i_5 = 2$ and $5 \nmid a_i$ for $i \in \mathcal{B}_3$. Lastly, we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{23, 73\}$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) := (2, 0)$, $\mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41\}$ and $\ell = \ell_4 = \sum_{p\in\mathcal{P}_4} \lceil k/p \rceil$. By Lemma 5, we see that $M = \{23, 29, 35, 36, 50, 53, 56, 65, 71, 74\}$ is covered by $\mathcal{P}_4$, $i_3 = 2$, $i_{41} = 36$, $B = \{5, 13, 14, 21, 28, 41, 45, 49, 59, 61, 63, 68, 69, 70, 73, 75, 76\}$ and hence $a_i \in \{1, 2, 7, 14\}$ for $i \in B$. By taking $\mathcal{J} = B$, we have $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^2 = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

$$\mathcal{I}_3^0 = \{5, 14, 41, 59, 68\}, \quad \mathcal{I}_3^1 = \{13, 28, 49, 61, 70, 73, 76\},$$
$$\mathcal{I}_3^2 = \{21, 45, 63, 69, 75\}$$

and

$$\mathcal{I}_5^+ = \{13, 21, 28, 41, 61, 63, 68, 73, 76\}, \quad \mathcal{I}_5^- = \{5, 14, 45, 49, 59, 69, 70, 75\}.$$

Thus

$$\mathcal{J}_1 = \{13, 28, 61, 73, 76\}, \quad \mathcal{J}_2 = \{49, 70\}, \quad \mathcal{J}_3 = \{21, 63\}, \quad \mathcal{J}_4 = \{45, 69, 75\},$$

and hence $a_{13} = a_{28} = a_{61} = a_{73} = a_{76} = 1$, $a_{49} = a_{70} = 7$, $a_{21} = a_{63} = 14$, $a_{45} = a_{69} = a_{75} = 2$ by (17). Further, we get $a_{41} = a_{68} = 1$ and $a_5 = a_{59} = 2$ by residues modulo 5. Since $\left(\frac{1}{79}\right) = \left(\frac{2}{79}\right) = 1$, we see that $\left(\frac{a_i}{71}\right) = 1$ for $i \in \{5, 13, 28, 41, 45, 59, 61, 68, 69, 75, 76\}$, which is not valid by the possibilities for i_{79} given by (23). The other cases are excluded similarly.

3.9. *The case* $k = 83$. We have $q_1 = 37$, $q_2 = 83$ and $\mathcal{P}_1 = \{17, 23, 29, 31, 47, 53, 59, 61, 67, 71, 73\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by

$$(13, 4), (14, 5), (15, 6), (16, 7), (17, 8), (18, 9), (19, 10),$$
$$(20, 11), (21, 12), (22, 13), (23, 14), (24, 15), (25, 16), (26, 17).$$

These pairs are of the form $(i + 9, i)$ with $4 \leq i \leq 17$.

Let $(i_{37}, i_{83}) = (13, 4)$. We see that $\mathcal{P}_1 = \{17, 23, 29, 31, 47, 53, 59, 61, 67, 71, 73\}$, $\mathcal{M}_1 = \{0$, 2, 14, 16, 18, 19, 20, 25, 26, 28, 29, 34, 36, 40, 41, 53, 56, 58, 64, $70\}$, $\mathcal{B}_1 = \{1, 3, 5, 6, 7, 8, 9, 10, 11, 12, 15, 17, 21, 22, 23, 24, 27, 30, 31$, 32, 33, 35, 37, 38, 39, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 54, 55, 57, 59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, $82\}$, $i_{17} = 2$, $i_{23} = 18$, $i_{29} = 0$, $i_{31} = 25$ and $\{14, 16, 20, 26, 28, 34, 40\}$ is covered by $\{47, 53, 59, 61, 67, 71, 73\}$. Further, $p \nmid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. For each possibility $i_{73} \in \{14, 16, 20, 26, 28, 34, 40\}$, we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{37, 83\}$, $p_1 = 23$, $p_2 = 73$, $(i_1, i_2) := (18, i_{73})$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(23, 73) \setminus \mathcal{P}_0 = \{13, 19, 79\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 14$. Then $|\mathcal{I}'| = |\mathcal{B}_1| > 2\ell_2$. Thus the conditions of Corollary 1 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$, which is possible only if $i_{73} = 14$. Then $\mathcal{M}_2 = \{8, 9, 11, 22, 30, 35, 48, 49, 61, 68, 74\}$. Therefore $i_{13} = 9$, $i_{19} = 11$ and $i_{79} = 8$. This is not possible by applying the case $k = 73$ to $(n + 9d) \cdots (n + 81d)$. Similarly, for $(i_{37}, i_{83}) = (14, 5)$, we get $i_{73} = 15$, $i_{79} = 9$ and this is excluded by applying the case $k = 73$ to $(n + 10d) \cdots (n + 82d)$. For all the remaining cases, we continue similarly to find that $\mathcal{M}_2$ is not covered by $\mathcal{P}_2$ for the possible choices of i_{73}, and hence they are excluded.

3.10. *The case* $k = 89$. We have $q_1 = 79$, $q_2 = 89$ and $\mathcal{P}_1 = \{13, 17, 19, 23, 31, 47, 53, 71, 83\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by

$$(16, 6), (17, 7), (18, 8), (19, 9), (20, 10), (21, 11).$$

These pairs are of the form $(i + 10, i)$ with $6 \le i \le 11$.

Let $(i_{79}, i_{89}) = (16, 6)$. We see that $\mathcal{P}_1 = \{13, 17, 19, 23, 31, 47, 53, 71, 83\}$, $\mathcal{M}_1 = \{0$, 1, 2, 3, 4, 10, 12, 17, 19, 24, 26, 27, 30, 33, 38, 42, 43, 44, 48, 49, 56, 57, 61, 64, 69, 72, 76, 78, $82\}$, $\mathcal{B}_1 = \{5$, 7, 8, 9, 11, 13, 14, 15, 18, 20, 21, 22, 23, 25, 28, 29, 31, 32, 34, 35, 36, 37, 39, 40, 41, 45, 46, 47, 50, 51, 52, 53, 54, 55, 58, 59, 60, 62, 63, 65, 66, 67, 68, 70, 71, 73, 74, 75, 77, 79, 80, 81, 83, 84, 85, 86, 87, $88\}$, $i_{13} = 4$, $i_{17} = 10$, $i_{19} = 0$, $i_{23} = 3$, $i_{31} = 2$, $i_{47} = 1$ and $\{12, 24, 42\}$ is covered by $\{53, 71, 83\}$. Further, $p \nmid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{79, 89\}$, $p_1 = 31$, $p_2 = 89$, $(i_1, i_2) := (2, 6)$, $\mathcal{I} = \mathcal{B}_1$ and $\mathcal{P} = \mathcal{P}_2 := \Lambda(31, 89) \setminus \mathcal{P}_0 = \{7, 11, 41, 59, 73\}$. If $7 \nmid d$, we observe that there is at least one multiple of 7 among $n + (i_{13} + 13i)d$, $0 \le i \le 6$, and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil - 1 = 28$. Thus in all cases, we have $\ell \le \ell_2$ and $|\mathcal{I}'| = |\mathcal{B}_1| > 2\ell_2$. Therefore the conditions of Corollary 1 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$ and $\mathcal{B} =: \mathcal{B}_2$ with $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ having Property $\mathfrak{H}$. We find $\mathcal{M}_2 = \{7$, 11, 13, 22, 25, 29, 32, 36, 39, 40, 51, 53, 54, 60, 62, 67, 73, 74, 81, 84, $88\}$, $\mathcal{B}_2 = \{5$, 8, 9, 14, 15, 18, 20, 21, 23, 28, 31, 34, 35, 37, 41, 45, 46, 47, 50, 52, 55, 58, 59, 63, 65, 66, 68, 70, 71, 75, 77, 79, 80, 83, 85, 86, $87\}$, $i_7 = 4$, $i_{11} = 7$, $i_{41} = 13$ and $\{22, 36\}$ is covered by $\{59, 73\}$. Further, for $p \in \mathcal{P}_2$, $p \nmid a_i$ for $i \in \mathcal{B}_2 \setminus \{18\}$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{79, 89\}$, $p_1 = 41$, $p_2 = 79$, $(i_1, i_2) := (13, 16)$, $\mathcal{I} = \mathcal{B}_2 \setminus \{18\}$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(41, 79) \setminus \mathcal{P}_0 = \{37, 43, 61, 67\}$ and $\ell =$

$\ell_3 = \sum_{p\in\mathcal{P}_3}\lceil k/p\rceil = 10$. Then $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_2|-1 > 2\ell_3$. Thus the conditions of Corollary 1 are satisfied and we have $\mathcal{M} =: \mathcal{M}_3$, $\mathcal{B} =: \mathcal{B}_3$ such that $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ has Property $\mathfrak{H}$. We get $\mathcal{M}_3 = \{9, 21, 28, 34, 52, 58\}$, $\mathcal{B}_3 = \{5, 8, 14, 15, 20, 23, 31, 35, 37, 41, 45, 46, 47, 50, 55, 59, 63, 65, 66, 68, 70, 71, 75, 77, 79, 80, 83, 85, 86, 87\}$, $i_{37} = 21, i_{43} = 9$ and $\{28, 34\}$ is covered by $\{61, 67\}$. Therefore $p \in \{2, 3, 5, 29\}$ whenever $p \mid a_i$ for $i \in \mathcal{B}_3$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{79, 89\}$, $p_1 = 7$, $p_2 = 17$, $(i_1, i_2) := (4, 10)$, $\mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(7, 17)\backslash\mathcal{P}_0 = \{29\}$ and $\ell = \ell_4 = \lceil k/29\rceil = 4$. Then $|\mathcal{I}'| = |\mathcal{B}_3|-1$ since $46 \in \mathcal{B}_3$ and $|\mathcal{B}_3| - 1 > 2\ell_3$. By Corollary 1, we get $\mathcal{M} =: \mathcal{M}_4$ and $\mathcal{B} =: \mathcal{B}_4$ with $(\mathcal{M}_4, \mathcal{B}_4, \mathcal{P}_4, \ell_4)$ having Property $\mathfrak{H}$. We find $\mathcal{M}_4 = \{8, 37, 66\}$, $\mathcal{B}_4 = \{5, 14, 15, 20, 23, 31, 35, 41, 45, 47, 50, 55, 59, 63, 65, 68, 70, 71, 75, 77, 79, 80, 83, 85, 86, 87\}$, $i_{29} = 8$ and $P(a_i) \le 5$ for $i \in \mathcal{B}_4$. Now we get a contradiction by taking $k = 6$ and $(n+47d)(n+55d)(n+63d)(n+71d)(n+79d)(n+87d) = b'y'^2$. Similarly the pair $(i_{79}, i_{89}) = (17, 7)$ is excluded by applying $k = 6$ to $(n+48d)(n+56d)(n+64d)(n+72d)(n+80d)(n+88d)$. For all the remaining cases, we continue similarly to find that $\mathcal{M}_3$ is not covered by $\mathcal{P}_3$, and hence they are excluded. ■

4. Proof of Lemma 7. Assume that $Q_1 \nmid d$ and $Q_2 \nmid d$. Then, by taking the mirror image (4) of (2), there is no loss of generality in assuming that $0 \le i_{Q_1} < Q_1$, $0 \le i_{Q_2} \le \min(Q_2 - 1, (k-1)/2)$. Further, $i_{Q_2} \ge k - k'$ if $Q_2 = k$. Let $\mathcal{P}_0 = \{Q_0\}, p_1 = Q_1, p_2 = Q_2, (i_1, i_2) := (i_{Q_1}, i_{Q_2}), \mathcal{I} = [0, k) \cap \mathbb{Z}$ and $\mathcal{P} = \mathcal{P}_1 := \Lambda(Q_1, Q_2) \setminus \mathcal{P}_0$. Then $|\mathcal{I}'| \ge k - \lceil k/Q_1\rceil - \lceil k/Q_2\rceil$ and $\ell \le \ell_1$ where $\ell_1 = \sum_{p\in\mathcal{P}_1}\lceil k/p\rceil$. In fact we can take $\ell_1 = \sum_{p\in\mathcal{P}_1}\lceil k/p\rceil - 1$ if $(k, Q_0) = (79, 23)$ or $(k, Q_0) = (59, 29)$ with $i_7 \le 2$ by considering multiples of $13, 11$ or $19, 7, 11$, respectively.

Let $(k, Q_0) \ne (79, 73)$. Then $\ell_1 < \frac{1}{2}|\mathcal{I}'|$. We observe that $\mathfrak{i}(\mathcal{P}_0) = 0$ for $i \in \mathcal{I}'$ since $Q_0 \mid d$, and by Corollary 1, we get $\mathcal{M} =: \mathcal{M}_1$, $\mathcal{B} =: \mathcal{B}_1$ such that $(\mathcal{M}_1, \mathcal{B}_1, \mathcal{P}_1, \ell_1)$ has Property $\mathfrak{H}$. We now restrict to all such pairs (i_{Q_1}, i_{Q_2}) with $|\mathcal{M}_1| \le \ell_1$ and $\mathcal{M}_1$ covered by $\mathcal{P}_1$. These pairs are given by

k	Q_0	(Q_1, Q_2)	(i_{Q_1}, i_{Q_2})
29	19	$(7, 17)$	$(0, 0), (0, 11)$
37	19 or 29	$(7, 17)$	$(0, 0), (1, 2)$
47	29	$(7, 17)$	$(0, 0), (4, 12)$
59	29	$(7, 17)$	$(1, 1), (1, 6)$
71	43	$(53, 67)$	$(0, 0)$
89	79	$(23, 73)$	$(0, 0), (19, 15)$

Let $(k, Q_0) = (79, 73)$ and $(Q_1, Q_2) = (53, 67)$. We apply Lemma 5 to derive that either $|\mathcal{I}_1| \le \ell_1$, $\mathcal{I}_1$ is covered by $\mathcal{P}_1$, $\mathfrak{i}(\mathcal{P}_1)$ is even for $i \in \mathcal{I}_2$, or

$|\mathcal{I}_2| \le \ell_1$, $\mathcal{I}_2$ is covered by $\mathcal{P}_1$, $\mathfrak{i}(\mathcal{P}_1)$ is even for $i \in \mathcal{I}_1$. We compute $\mathcal{I}_1$, $\mathcal{I}_2$ and we find that both $\mathcal{I}_1$ and $\mathcal{I}_2$ are not covered by $\mathcal{P}_1$ for each pair (i_{53}, i_{67}) with $0 \le i_{53} < 53$, $0 \le i_{67} \le (k-1)/2$.

Let $(k, Q_0) = (37, 29)$, $(Q_1, Q_2) = (7, 17)$ and $(i_7, i_{17}) = (1, 2)$. Then $\mathcal{P}_1 = \{11, 13, 19, 23, 37\}$. We find that $\mathcal{M}_1 = \{3, 7, 10, 13, 14, 17, 23, 25\}$, $\mathcal{B}_1 = \{0, 4, 5, 6, 9, 11, 12, 16, 18, 20, 21, 24, 26, 27, 28, 30, 31, 32, 33, 34, 35\}$, $i_{11} = 3$, $i_{13} = 10$ and $\{7, 13, 17\}$ is covered by $\{19, 23, 37\}$. Further, $p \nmid a_i$ for $p \in \mathcal{P}_1$, $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{7, 17, 29\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (3, 10)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 10$. Thus $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_1| = 21 > 2\ell_2$. Then the conditions of Corollary 1 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$. We get $\mathcal{M}_2 = \{5, 6, 16, 21, 26, 31\}$, $\mathcal{B}_2 = \{0, 4, 9, 11, 12, 18, 20, 24, 27, 28, 30, 32, 33, 34, 35\}$, $i_5 = 1$, $31 \mid a_5$ and $5 \nmid a_{11}$. Also, $P(a_i) \le 3$ for $i \in B_2$ and $P(a_{31}) = 5$. Thus $P(a_{30} a_{31} \cdots a_{35}) \le 5$ and this is excluded by the case $k = 6$. The other cases for $k = 29, 37, 47$ are excluded similarly. Each possibility is excluded by the case $k = 6$ after showing $P(a_1 a_2 \cdots a_6) \le 5$ when $(k, Q_0) \in \{(29, 19), (37, 19), (37, 29), (47, 29)\}$, $(i_7, i_{17}) = (0, 0)$; $P(a_{22} a_{23} \cdots a_{27}) \le 5$ when $(k, Q_0) = (29, 19)$, $(i_7, i_{17}) = (0, 11)$; $P(a_{30} a_{31} \cdots a_{35}) \le 5$ when $(k, Q_0) = (37, 19)$, $(i_7, i_{17}) = (1, 2)$; and $P(a_{40} a_{41} \cdots a_{45}) \le 5$ when $(k, Q_0) = (47, 29), (i_7, i_{17}) = (4, 12)$.

Let $(k, Q_0) = (59, 29)$, $(Q_1, Q_2) = (7, 17)$ and $(i_7, i_{17}) = (1, 1)$. Then $\mathcal{P}_1 = \{11, 13, 19, 23, 37, 47, 59\}$. We find that $\mathcal{M}_1 = \{0, 12, 14, 20, 23, 24, 27, 30, 34, 38, 39, 40, 45, 47, 48, 53, 56, 58\}$, $\mathcal{B}_1 = \{2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 16, 17, 19, 21, 25, 26, 28, 31, 32, 33, 37, 41, 42, 44, 46, 49, 51, 54, 55\}$, $i_{11} = i_{13} = i_{19} = i_{23} = 1$ and $\{30, 38, 48\}$ is covered by $\{37, 47, 59\}$. Further, $p \nmid a_i$ for $p \in \mathcal{P}_1$, $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{7, 17, 29\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (1, 1)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31, 43\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil$. By Lemma 5, we get $M = \{6, 11, 16, 21, 31, 32, 41, 44, 46\}$, $i_5 = 1$, $31 \cdot 43 \mid a_{32} a_{44}$, and $\mathfrak{i}(\mathcal{P}_2)$ is even for $i \in B = \{2, 3, 4, 5, 7, 9, 10, 13, 17, 19, 25, 26, 28, 33, 37, 42, 49, 51, 54, 55\}$. Further, for $p \in \mathcal{P}_2$, $p \nmid a_i$ for $i \in B$. Finally we apply Lemma 5 with $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{7, 17, 29\}$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) := (1, 1)$, $\mathcal{I} = B$ and $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41, 53\}$. We get $M_1 = \{4, 7, 13, 25, 28, 42, 49, 54, 55\}$, which is covered by $\mathcal{P}_3$, $i_3 = 1$, $\{42, 54\}$ is covered by $\{41, 53\}$ and $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B_1 = \{2, 3, 5, 9, 10, 17, 19, 33, 37\}$. Hence $P(a_i) \le 2$ for $i \in B_1$. Since $\left(\frac{a_i}{29}\right) = \left(\frac{n}{29}\right)$ and $\left(\frac{2}{29}\right) \ne 1$, we see that $a_i = 1$ for $i \in B_1$. By taking $\mathcal{J} = B_1$, we derive that either $\mathcal{I}_5^+ = \emptyset$ or $\mathcal{I}_5^- = \emptyset$, which is a contradiction. The other case $(i_7, i_{17}) = (1, 6)$ is excluded similarly.

Let $(k, Q_0) = (71, 43)$, $(Q_1, Q_2) = (53, 67)$, $(i_{53}, i_{67}) = (0, 0)$. Then $\mathcal{P}_1 = \{7, 11, 13, 19, 23, 71\}$. We get $\mathcal{M}_1 = \{7, 11, 13, 14, 19, 21, 22, 23, 26, 28, 33, 35, 38, 39, 42, 43, 44, 46, 52, 55, 56, 57, 63, 65, 66, 69, 70\}$, $\mathcal{B}_1 = \{1, 2, 3, 4, 5, 6, 8, 9,$

$10, 12, 15, 16, 17, 18, 20, 24, 25, 27, 29, 30, 31, 32, 34, 36, 37, 40, 41, 45, 47, 48, 49, 50, 51, 54, 58, 59, 60, 61, 62, 64, 68\}$, $i_7 = i_{11} = i_{13} = i_{19} = i_{23} = 0$, $i_{71} = 43$. Further, for $p \in \mathcal{P}_1$, $p \nmid a_i$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{43, 53, 67\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (0, 0)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 17, 29, 31, 37, 47, 59, 61\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil$. By Lemma 5, we see that $M = \{5, 10, 15, 17, 20, 29, 30, 31, 34, 37, 40, 45, 47, 51, 58, 59, 60, 61, 62, 68\}$ is covered by $\mathcal{P}_2$ and $\mathfrak{i}(\mathcal{P}_2)$ is even for $i \in B = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 25, 27, 32, 36, 41, 48, 49, 50, 54, 64\}$. We get $i_5 = i_{17} = i_{29} = i_{31} = 0$, and $\{37, 47, 59, 61\}$ is covered by $\{37, 47, 59, 61\}$. Thus $37 \cdot 47 \cdot 59 \cdot 61 \mid a_{37} a_{47} a_{59} a_{61}$. Further, $p \nmid a_i$ for $i \in B$ and $p \in \mathcal{P}_2$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{43, 53, 67\}$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) := (0, 0)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41\}$ and $\ell = \ell_3 = \sum_{p \in \mathcal{P}_3} \lceil k/p \rceil$. By Lemma 5, we see that $M_1 = \{3, 6, 12, 24, 27, 41, 48, 54\}$ is covered by $\mathcal{P}_3$ and $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B_1 = \{1, 2, 4, 8, 9, 16, 18, 32, 36, 49, 64\}$. Thus $i_3 = 0$, implying $i_{41} = 0$ and $p = 2$ whenever $p \mid a_i$ for $i \in B_1$. By taking $\mathcal{J} = B_1$, we have $B_1 = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

$$\mathcal{I}_5^+ = \{1, 4, 9, 16, 36, 49, 64\}, \quad \mathcal{I}_5^- = \{2, 8, 18, 32\}.$$

Thus $a_i = 1$ for $i \in \mathcal{I}_5^+$ and $a_i = 2$ for $i \in \mathcal{I}_5^-$ since $a_i \in \{1, 2\}$ for $i \in B_1$. This is a contradiction since $43 \mid d$, $\left(\frac{a_i}{43}\right) = \left(\frac{n}{43}\right)$ and $\left(\frac{1}{43}\right) \neq \left(\frac{2}{43}\right)$.

Let $k = 89$, $Q_0 = 79$, $(Q_1, Q_2) = (23, 73)$, $(i_{23}, i_{73}) = (19, 15)$. Then $\mathcal{P}_1 = \{13, 19, 29, 31, 37, 47, 59, 61, 67, 79, 89\}$. We find that $\mathcal{M}_1 = \{1, 9, 10, 12, 14, 21, 23, 26, 27, 29, 30, 31, 36, 41, 49, 50, 51, 57, 59, 62, 69, 75\}$, $\mathcal{B}_1 = \{0, 2, 3, 4, 5, 6, 7, 8, 11, 13, 16, 17, 18, 20, 22, 24, 25, 28, 32, 33, 34, 35, 37, 38, 39, 40, 43, 44, 45, 46, 47, 48, 52, 53, 54, 55, 56, 58, 60, 61, 63, 64, 66, 67, 68, 70, 71, 72, 73, 74, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87\}$, $i_{13} = 10$, $i_{19} = 12$, $i_{29} = 1$, $i_{31} = 26$, $i_{37} = 14$ and $\{9, 21, 27, 29, 41\}$ is covered by $\{47, 59, 61, 67, 89\}$. Thus $i_{89} \in \{9, 21, 27, 29, 41\}$. Further, for $p \in \mathcal{P}_1$, $p \nmid a_i$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{23, 73, 79\}$, $p_1 = 19$, $p_2 = 29$, $(i_1, i_2) := (12, 1)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(19, 29) \setminus \mathcal{P}_0 = \{11, 17, 43, 53, 71\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 22$. Thus $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_1| > 2\ell_2$. By Corollary 1, we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has Property $\mathfrak{H}$. We get $\mathcal{M}_2 = \{0, 2, 3, 11, 17, 20, 22, 33, 35, 37, 44, 45, 54, 55, 66, 71, 77\}$, $\mathcal{B}_2 = \{4, 5, 6, 7, 8, 13, 16, 18, 24, 25, 28, 32, 34, 38, 39, 40, 43, 46, 47, 48, 52, 53, 56, 58, 60, 61, 63, 64, 67, 68, 70, 72, 73, 74, 76, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87\}$, $i_{11} = 0$, $i_{17} = 3$, $i_{43} = 2$ and $\{17, 35\}$ is covered by $\{53, 71\}$. Further, $p \nmid a_i$ for $i \in \mathcal{B}_2$ and $p \in \mathcal{P}_2$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{23, 73, 79\}$, $p_1 = 11$, $p_2 = 13$, $(i_1, i_2) := (0, 10)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5\}$ and $\ell = \ell_3 = \sum_{p \in \mathcal{P}_2} \lceil k/p \rceil = 18$. Thus $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_2| > 2\ell_3$. Then the conditions of Corollary 1 are satisfied and we have $\mathcal{M} =: \mathcal{M}_3$, $\mathcal{B} =: \mathcal{B}_3$ with $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ having Property $\mathfrak{H}$. We get $\mathcal{M}_3 = \{8, 18, 28, 43, 48, 53, 58, 68, 73, 78, 83\}$, $\mathcal{B}_3 = \{4, 5, 6, 7, 13, 16, 24, 25, 32, 34, 38, 39, 40, 46, 47, 52, 56, 60, 61, 63, 64, 67, 70, 72, 74, 76,$

79, 80, 81, 82, 84, 85, 86, 87}, $i_5 = 3$. Lastly, we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{23, 73, 79\}$, $p_1 = 5$, $p_2 = 11$, $(i_1, i_2) := (3, 0)$, $\mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41\}$ and $\ell = \ell_4 = \sum_{p\in\mathcal{P}_4} \lceil k/p \rceil$. By Lemma 5, we see that $M = \{4, 6, 34, 40, 46, 47, 61, 64, 67, 76, 82, 85\}$ is covered by $\mathcal{P}_4$ and $\mathfrak{i}(\mathcal{P}_4)$ is even for $i \in B = \{5, 7, 16, 24, 25, 32, 39, 52, 56, 60, 70, 72, 74, 79, 80, 81, 84, 86, 87\}$. Thus $i_3 = 1$, $i_{41} = 6$ and $p \in \{2, 7, 83\}$ whenever $p \mid a_i$ for $i \in B$. Since $79 \mid d$, we see that $a_i \in \{1, 2, 83, 2 \cdot 83\}$ or $a_i \in \{7, 14, 7 \cdot 83, 14 \cdot 83\}$ for $i \in B$. The latter possibility is excluded since $7 \nmid i - i'$ for all $i, i' \in B$. By taking $\mathcal{J} = B$, we have $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

$$\mathcal{I}_5^+ = \{7, 24, 32, 39, 52, 72, 74, 79, 84, 87\},$$
$$\mathcal{I}_5^- = \{5, 16, 25, 56, 60, 70, 80, 81, 86\}.$$

Then we observe that either $a_i \in \{1, 2 \cdot 83\}$ for $i \in \mathcal{I}_5^+$ and $a_i \in \{2, 83\}$ for $i \in \mathcal{I}_5^-$ or *vice versa*. This is not possible by parity argument. The other case $(i_{23}, i_{73}) = (0, 0)$ is excluded similarly. ■

5. Proof of Lemma 8. Let $7 \le k \le 97$ be primes. Suppose that the assumptions of Lemma 8 are satisfied. Assume that $q_1 \mid d$ or $q_2 \mid d$ and we shall arrive at a contradiction. We divide the proof into Subsections 5.1 and 5.2.

5.1. *The cases* $7 \le k \le 23$. We take $q = 5$ in (7) and (8). We may suppose that $5 \mid d$ if $k = 7, 11$ and $11 \mid d$ if $k = 13$. Let $5 \mid d$. Then

$$S \subseteq \{1, 6\} \quad \text{or} \quad S \subseteq \{2, 3\} \tag{24}$$

according as $\left(\frac{n}{5}\right) = 1$ or -1, respectively. Thus (24) holds if $k = 7, 11$. Let $11 \mid d$. Then

$$S \subseteq \{1, 3, 5, 15\} \quad \text{or} \quad S \subseteq \{2, 6, 10, 30\} \tag{25}$$

according as $\left(\frac{n}{11}\right) = 1$ or -1, respectively. Let $13 \mid d$. Then

$$S \subseteq \{1, 3, 10, 30\} \quad \text{or} \quad S \subseteq \{2, 5, 6, 15\} \tag{26}$$

according as $\left(\frac{n}{13}\right) = 1$ or -1, respectively. Thus either (25) or (26) holds if $13 \le k \le 23$.

By observing that a_i's divisible by a prime p can occur in at most $\lceil k/p \rceil$ terms, we have

$$|T_1| \le t_1' := \begin{cases} \sum_{p>5} \lceil k/p \rceil & \text{if } k = 7, 11, \\ \sum_{p>5} \lceil k/p \rceil - 2 & \text{if } 13 \le k < 23, \\ \sum_{p>5} \lceil k/p \rceil - 3 & \text{if } k = 23, \end{cases} \tag{27}$$

where the sum is taken over all $p \le k$. For the last sum, we observe that 7 and 11 together divide at most six a_i's when $k = 23$. We divide the proof into four cases.

Case I. Let $2\nmid d$ and $3\nmid d$. From (24)–(26), (10) and Lemma 1, we get

$$|T| \le t_1 := \begin{cases} \max(f_1(k,1,0)+f_1(k,6,0), f_1(k,2,0)+f_1(k,3,0)) + \lceil k/4\rceil \\ \hfill \text{if } k=7,11, \\ f_1(k,1,0)+f_1(k,3,0)+f_1(k,5,0)+f_1(k,15,0)+\lceil k/4\rceil \\ \hfill \text{if } k>11, \end{cases}$$

since $f_1(k,a,\delta)$ is a nonincreasing function of a and $\sum_{a\in R}\nu_{\mathrm{e}}(a) \le \lceil k/4\rceil$. We check that $k = |T|+|T_1| \le t_1 + t_1' < k$, a contradiction.

Thus we have either $2\,|\,d$ or $3\,|\,d$. Let $k = 7, 11$. If $2\,|\,d$, then $S\subseteq\{1\}$ or $S\subseteq\{3\}$. If $3\,|\,d$, we have $S\subseteq\{1\}$ or $S\subseteq\{2\}$. By Lemma 2, we get $|T|\le(k-1)/2$. We check that $k=|T|+|T_1|\le(k-1)/2+t_1'<k$ by (27). This is a contradiction. From now on, we may also suppose that $13\le k\le 23$.

Case II. Let $2\,|\,d$ and $3\nmid d$. Then $S\subseteq\{1,3,5,15\}$ if $11\,|\,d$ and $S\subseteq\{1,3\}$ or $S\subseteq\{5,15\}$ if $13\,|\,d$. Let $2\,\|\,d$. From (10) and Lemma 1 with $\delta=1$, we get

$$|T|\le F(k,1,1)+F(k,3,1)+F(k,5,1)+F(k,15,1) =: t_2.$$

Let $4\,\|\,d$. From $a_i\equiv n \pmod 4$, we see that $S\subseteq\{1,5\}$ or $S\subseteq\{3,15\}$ if $11\,|\,d$, and either $S=\emptyset$ or $S=\{1\},\{3\},\{5\}$ or $\{15\}$ if $13\,|\,d$. Therefore

$$|T|\le F(k,1,2)+F(k,5,2) =: t_3$$

by Lemma 1 with $\delta=2$. Let $8\,|\,d$. Then $a_i\equiv n \pmod 8$ and Lemma 1 with $\delta=3$ imply

$$|T|\le F(k,1,3) =: t_4.$$

Thus $|T|\le$max(t_2,t_3,t_4). This with (27) contradicts (9).

Case III. Let $2\nmid d$ and $3\,|\,d$. From $a_i\equiv n \pmod 3$, we see that either $S=\emptyset$ or $S=\{1\},\{2\},\{5\}$ or $\{10\}$ if $11\,|\,d$, and $S\subseteq\{1,10\}$ or $S\subseteq\{2,5\}$ if $13\,|\,d$. By (10) and Lemma 1, we get

$$|T|\le F(k,1,0)+F(k,5,0),$$

which together with (27) contradicts (9).

Case IV. Let $2\,|\,d$ and $3\,|\,d$. Then $S\subseteq\{1\},\{5\}$. By Lemma 2, we get $|T|\le(k-1)/2$. We check that $k=|T|+|T_1|\le(k-1)/2+t_1'<k$, a contradiction.

5.2. *The cases $k\ge 29$.* Let $29\le k\le 59$ and $19\,|\,d$. Then by Lemma 7 with $Q_0=19$, we get $7\,|\,d$ or $17\,|\,d$. Thus we get a prime pair $(Q,Q')=(7,19)$ or $(Q,Q')=(17,19)$ such that $QQ'\,|\,d$. Similarly we get $(Q,Q')=(7,29)$ or $(Q,Q')=(17,29)$ with $QQ'\,|\,d$ when $31\le k\le 59$ and $29\,|\,d$. Let $k=71$. Then we have either $43\,|\,d$, $67\,|\,d$ or $43\,|\,d$, $67\nmid d$ or $43\nmid d$, $67\,|\,d$. We get a prime pair $(Q,Q')=(43,67)$ with $QQ'\,|\,d$ if $43\,|\,d$, $67\,|\,d$. If $43\,|\,d$, $67\nmid d$, we deduce from Lemma 7 with $Q_0=43$ that $53\,|\,d$ and we take $(Q,Q')=(43,53)$ such that $QQ' \mid d$. If $43 \nmid d$, $67 \mid d$, we find from Lemma 7 with $Q_0 = 67$ that $53 \mid d$ and we take $(Q, Q') = (53, 67)$ such that $QQ' \mid d$. Similar prime pairs (Q, Q') with $QQ' \mid d$ for each $61 \le k \le 97$ are given in the table below. For $q \le 17$, we see that

$$(28)\qquad |T_1| \le \sum_{\substack{p>q\\ p\ne Q,Q'}} \left\lceil \frac{k}{p} \right\rceil \le t_2' := \begin{cases} \sum_{p>q}\lceil k/p\rceil - 2 & \text{if } 29 \le k \le 61,\\ \sum_{p>q}\lceil k/p\rceil - 4 & \text{if } 61 < k < 97,\\ \sum_{p>q}\lceil k/p\rceil - 7 & \text{if } k = 97,\end{cases}$$

where the sum is taken over primes $\le k$.

k	(Q, Q')	$S \subseteq S'$ with S' given by one of
$29 \le k \le 59$	$(7, 19), (7, 29)$	$\{1, 30\}, \{2, 15\}, \{3, 10\}, \{5, 6\}$
$29 \le k \le 59$	$(17, 19), (17, 29)$	$\{1, 30, 35, 42\}, \{2, 15, 21, 70\}, \{3, 10, 14, 105\}, \{5, 6, 7, 210\}$
61	$(11, 59)$	$\{1, 3, 5, 15\}, \{2, 6, 10, 30\}, \{7, 21, 35, 105\}, \{14, 42, 70, 210\}$
67, 71	$(43, 53)$	$\{1, 6, 10, 15\}, \{2, 3, 5, 30\}, \{7, 42, 70, 105\}, \{14, 21, 35, 210\}$
71	$(43, 67)$	See (29)
71	$(53, 67)$	$\{1, 6, 10, 15\}, \{2, 3, 5, 30\}, \{7, 42, 70, 105\}, \{14, 21, 35, 210\}$
73	$(23, 53)$	$\{1, 6, 70, 105\}, \{2, 3, 35, 210\}, \{5, 14, 21, 30\}, \{7, 10, 15, 42\}$
73	$(23, 67)$	$\{1, 6, 35, 210\}, \{2, 3, 70, 105\}, \{5, 7, 30, 42\}, \{10, 14, 15, 21\}$
79	$(23, 53), (53, 73)$	$\{1, 6, 70, 105\}, \{2, 3, 35, 210\}, \{5, 14, 21, 30\}, \{7, 10, 15, 42\}$
79	$(23, 67), (67, 73)$	$\{1, 6, 35, 210\}, \{2, 3, 70, 105\}, \{5, 7, 30, 42\}, \{10, 14, 15, 21\}$
83	$(23, 37), (37, 73)$	$\{1, 3, 70, 210\}, \{2, 6, 35, 105\}, \{5, 14, 15, 42\}, \{7, 10, 21, 30\}$
89	$(23, 79), (73, 79)$	$\{1, 2, 105, 210\}, \{3, 6, 35, 70\}, \{5, 10, 21, 42\}, \{7, 14, 15, 30\}$
97	$(23, 37), (23, 83)$	$\{1, 3, 70, 210\}, \{2, 6, 35, 105\}, \{5, 14, 15, 42\}, \{7, 10, 21, 30\}$

CASE I. Let $2 \nmid d$ and $3 \nmid d$. In (7) and (8) we take $q = 11$ if $k = 71$, $(Q, Q') = (43, 67)$ and $q = 7$ otherwise. From $\left(\frac{a_i}{Q}\right) = \left(\frac{n}{Q}\right)$ and $\left(\frac{a_i}{Q'}\right) = \left(\frac{n}{Q'}\right)$, we get $S \subseteq S' = \left\{s : s \text{ squarefree}, P(s) \le q, \left(\frac{s}{Q}\right) = \left(\frac{n}{Q}\right), \left(\frac{s}{Q'}\right) = \left(\frac{n}{Q'}\right)\right\}$. By considering $\left(\left(\frac{n}{Q}\right), \left(\frac{n}{Q'}\right)\right) = (1, 1)$, $(1, -1)$, $(-1, 1)$ and $(-1, -1)$, we get four possibilities for S'. For each value of k, the above table shows (Q, Q') and S'. For $k = 71$, $(Q, Q') = (43, 67)$, we get $S \subseteq S'$ with S' given by one of

$$(29)\quad \begin{array}{l}\{1, 6, 10, 14, 15, 21, 35, 210\}, \{2, 3, 5, 7, 30, 42, 70, 105\},\\ \{11, 66, 110, 154, 165, 231, 385, 2310\}, \{22, 33, 55, 77, 330, 462, 770, 1155\}.\end{array}$$

From the possibilities for $S \subseteq S'$ given by the table, (10) and Lemma 1, we get

$$|T| \le t_5 := \max \sum_{s \in S'} F(k, s, 0),$$

where the maximum is taken over all the four choices of S'. This with (28) gives $|T| + |T_1| \le t_5 + t_2' < k$, contradicting (9).

Case II. Let $2 \mid d$ and $3 \nmid d$. We take $q = 7$ for $2 \parallel d$, $4 \parallel d$ and $q = 11$ for $8 \mid d$.

Let $2 \parallel d$. Then $S \subseteq \{1, 3, 5, 7, 15, 21, 35, 105\} =: S_2$. From (10) and Lemma 1 with $\delta = 1$, we get

$$|T| \le \sum_{s \in S_2} F(k, s, 1) =: t_6.$$

Let $4 \parallel d$. Then we see that either $S \subseteq \{1, 5, 21, 105\} =: S_{41}$ or $S \subseteq \{3, 7, 15, 35\} =: S_{42}$. From (10) and Lemma 1 with $\delta = 2$, we get

$$|T| \le \max_{i=1,2} \sum_{s \in S_{4i}} F(k, s, 2) =: t_7.$$

Hence, if $8 \nmid d$, then $|T| \le \max(t_6, t_7)$. This with (28) implies $|T| + |T_1| \le \max(t_6, t_7) + t_2' < k$, contradicting (9).

Let $8 \mid d$. Then we see from $a_i \equiv n \pmod 8$ that $S \subseteq \{1, 33, 105, 385\} =: S_{81}$ or $S \subseteq \{3, 11, 35, 1155\} =: S_{82}$ or $S \subseteq \{5, 21, 77, 165\} =: S_{83}$ or $S \subseteq \{7, 15, 55, 231\} =: S_{84}$. Then

$$|T| \le \max_{1 \le i \le 4} \sum_{s \in S_{8i}} F(k, s, 3) =: t_8$$

by Lemma 1 with $\delta = 3$. This with (28) implies $|T| + |T_1| \le t_8 + t_2' < k$, a contradiction.

Case III. Let $2 \nmid d$ and $3 \mid d$. We take $q = 11$. Then by modulo 3, we get either $S \subseteq \{1, 7, 10, 22, 55, 70, 154, 385\} =: S_{31}$ or $S \subseteq \{2, 5, 11, 14, 35, 77, 110, 770\} =: S_{32}$. By (10) and Lemma 1, we get

$$|T| \le \max_{i=1,2} \sum_{s \in S_{3i}} F(k, s, 0) =: t_9.$$

This together with (28) contradicts (9).

Case IV. Let $2 \mid d$ and $3 \mid d$. Let $2 \parallel d$. We take $q = 7$. Then we see that either $S \subseteq \{1, 7\}$ or $S \subseteq \{5, 35\}$. By (10) and Lemma 1, we get $|T| \le F(k, 1, 1) + F(k, 7, 1)$, which together with (28) contradicts (9).

Let $4 \parallel d$. We take $q = 13$. From $a_i \equiv n \pmod{12}$, we see that

$$\begin{aligned} S \subseteq S' \in \mathfrak{S} := \{&\{1, 13, 385, 5005\}, \{5, 65, 77, 1001\}, \\ &\{7, 55, 91, 715\}, \{11, 35, 143, 455\}\}. \end{aligned}$$

Then

$$|T| \le \max_{S' \in \mathfrak{S}} \sum_{s \in S'} F(k, s, 2),$$

which together with (28) contradicts (9).

Let $8\,|\,d$. We take $q = 17$. From $a_i \equiv n \pmod{24}$, we see that $S \subseteq S' = \{1, 385, 1105, 17017\}$ or $S \subseteq S'' \in \mathfrak{S}_1$ where $\mathfrak{S}_1$ is the union of sets

$$\begin{aligned}&\{5, 77, 221, 85085\}, \{7, 55, 2431, 7735\},\\&\{11, 35, 1547, 12155\}, \{13, 85, 1309, 5005\}, \{17, 65, 1001, 6545\},\\&\{91, 187, 595, 715\}, \{119, 143, 455, 935\}.\end{aligned}$$

Let $S \subseteq S'' \in \mathfrak{S}_1$. Then

$$|T| \le \max_{S'' \in \mathfrak{S}_1} \sum_{s \in S''} F(k, s, 3) =: t_{10}.$$

Let $S \subseteq S'$. By Lemma 2, we get $\nu(1) \le (k-1)/2$. This together with $\nu(1105) + \nu(17017) \le 1$ by $13 \cdot 17\,|\,\gcd(1105, 17017)$ and $\nu(385) \le 1$ by Lemma 1 gives $|T| \le (k-1)/2 + 2$. Therefore $|T| \le \max(t_{10}, (k-1)/2 + 2)$, which with (28) contradicts (9). ∎

6. Proof of Theorem 4. Let $k = 7$. By the case $k = 6$, we may assume that $7 \nmid d$. Now the assertion follows from Lemmas 8 and 6. Let $k = 8$. Then by applying the case $k = 7$ twice to $n(n+d)\cdots(n+6d) = b'y'^2$ and $(n+d)\cdots(n+7d) = b''y''^2$, we get

$$\begin{aligned}(a_0, \dots, a_6), (a_1, \dots, a_7)&\\ \in \{&(2,3,1,5,6,7,2), (3,1,5,6,7,2,1), (1,5,6,7,2,1,10),\\ &(2,7,6,5,1,3,2), (1,2,7,6,5,1,3), (10,1,2,7,6,5,1)\}.\end{aligned}$$

This gives $(a_0, \dots, a_7) = (2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10)$ or their mirror images and the assertion follows. Let $k = 9$. By applying the case $k = 8$ twice to $n(n+d)\cdots(n+7d) = b'y'^2$ and $(n+d)\cdots(n+8d) = b''y''^2$, we get the result. Let $k = 10$. By applying $k = 9$ twice, we get $(a_0, a_1, \dots, a_8), (a_1, a_2, \dots, a_8, a_9) \in \{(2,3,\dots,1,10), (10,1,\dots,3,2)\}$, which is not possible.

Let $k \ge 11$ and $k' < k$ be consecutive primes. We suppose that Theorem 4 is valid with k replaced by k'. Let $k\,|\,d$. Then $\left(\frac{a_i}{k}\right) = \left(\frac{n}{k}\right)$ for all $0 \le i < k$. By applying the case $k = k'$ to $n(n+d)\cdots(n+(k'-1)d) = b'y'^2$ with $P(b') \le k'$, we get $k' \le 23$ and $1, 2, 3, 5 \in \{a_0, a_1, \dots, a_{k'-1}\}$ in view of (5) and (6). Therefore $\left(\frac{2}{k}\right) = \left(\frac{3}{k}\right) = \left(\frac{5}{k}\right) = 1$, which is not possible.

Thus we may assume that $k \nmid d$ and $k\,|\,n + id$ for some $0 \le i \le (k-1)/2$ by considering the mirror image (4) of (2) whenever Theorem 4 holds at k'. We shall use this assertion without reference in the proof of Theorem 4.

Let $k = 11$. By Lemmas 8 and 6, we see that $11\,|\,n + id$ for $0 \le i \le 3$. If $11\,|\,n$, the assertion follows by the case $k = 10$. Let $11\,|\,n + d$. We consider $(n+2d)\cdots(n+10d) = b'y'^2$ with $P(b') \le 7$ and the case $k = 9$ to get $(a_2, a_3, \dots, a_{10}) \in \{(2,3,1,5,6,7,2,1,10), (10,1,2,7,6,5,1,3,2)\}$. The first possibility is excluded since $1 = \left(\frac{14}{11}\right) = \left(\frac{a_2 a_7}{11}\right) = \left(\frac{1\cdot 6}{11}\right) = -1$. For the second possibility, we observe $P(a_0) \le 5$ since $\gcd(a_0, 7\cdot 11) = 1$ and this is excluded by the case $k = 6$ applied to $n(n+2d)(n+4d)(n+6d)(n+8d)\cdot(n+10d)$. Let $11 \mid n+2d$. Then by the case $k = 8$, we have $(a_3, a_4, \ldots, a_{10}) \in \{(2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10), (1,2,7,6,5,1,3,2), (10,1,2,7,6,5,1,3)\}$. The first three possibilities are excluded by considering the values of the Legendre symbol mod 11 at a_3, a_8, at a_3, a_4 and at a_3, a_5, respectively. If the last possibility holds, then $a_0 = 1$ since $\gcd(a_0, 2\cdot 3\cdot 5\cdot 7\cdot 11) = 1$, and this is not possible since $1 = \left(\frac{a_0 a_4}{11}\right) = \left(\frac{(-2)2}{11}\right) = -1$. Let $11 \mid n+3d$. We consider $(n+4d)\cdots(n+10d) = b'y'^2$ with $P(b') \le 7$ and the case $k = 7$ to infer that $(a_4, \ldots, a_{10}) \in \{(2,3,1,5,6,7,2), (3,1,5,6,7,2,1), (1,5,6,7,2,1,10), (2,7,6,5,1,3,2), (1,2,7,6,5,1,3), (10,1,2,7,6,5,1)\}$, which is not possible as above. This completes the proof for $k = 11$. The assertion for $k = 12$ follows from that of $k = 11$.

Let $k = 13$. Then the assertion follows from Lemmas 8, 6 and the case $k = 11$. Let $k = 14$. By applying the case $k = 13$ to $n(n+d)\cdots(n+12d) = b'y'^2$ and $(n+d)\cdots(n+13) = b''y''^2$, we get the assertion. Let $k = 15$. Then applying the case $k = 14$ both to $n(n+d)\cdots(n+13d)$ and $(n+d)\cdots(n+14d)$ gives the result. For $k = 16$ the assertion follows from the case $k = 15$.

Let $k = 17$. Then $17 \mid n+2d$ or $17 \mid n+3d$ by Lemmas 8, 6 and the case $k = 15$. Let $17 \mid n+2d$. Then by applying the case $k = 14$ to $(n+3d)\cdots(n+16d) = b'y'^2$ with $P(b') \le 13$, we get $(a_3, a_4, \ldots, a_{16}) \in \{(3,1,\ldots,15,1), (1,15,\ldots,1,3)\}$. The first possibility is excluded by considering the Legendre symbol mod 17 at a_3, a_4. For the second, we observe that $\gcd(a_1, 7\cdot 11\cdot 13\cdot 17) = 1$, which is not possible by the case $k = 6$ applied to $(n+d)\cdot(n+4d)(n+7d)(n+10d)(n+13d)(n+16d)$. Let $17 \mid n+3d$. By considering $(n+4d)\cdots(n+16d) = b'y'^2$ with $P(b') \le 13$, it follows from the case $k = 13$ that $(a_4, \ldots, a_{16}) \in \{(3,1,\ldots,14,15), (1,5,\ldots,15,1), (15,14,\ldots,1,3), (1,15,\ldots,5,1)\}$. The first three possibilities are excluded by considering the Legendre symbol mod 17 at a_4, a_5. If the last possibility holds, we observe that $a_1 = 1$ since $\gcd(a_1, \prod_{p\le 17} p) = 1$ and then $1 = \left(\frac{a_1 a_4}{17}\right) = \left(\frac{(-6)(-3)}{17}\right) = -1$, a contradiction. The assertion for $k = 18$ follows from that for $k = 17$.

Let $k = 19$. Then the assertion follows from Lemmas 8, 6 and the case $k = 17$. By applying the case $k = 19$ twice to $n(n+d)\cdots(n+18d)$ and $(n+d)\cdots(n+18d)(n+19d)$, the assertion for $k = 20$ follows and this also implies the cases $k = 21, 22$.

Let $k = 23$. We see from Lemmas 8, 6 and the case $k = 20$ that 23 divides $n+3d$. We consider the case $k = 19$ and $(n+4d)\cdots(n+22d) = b'y'^2$ with $P(b') \le 19$ to get $(a_4, a_5, \ldots, a_{22}) = (1,5,\ldots,21,22)$ or $(22,21,\ldots,5,1)$. By considering the values of the Legendre symbol mod 23 at a_4 and a_5, we may assume the second possibility. Now $P(a_2) \le 11$ and this is not possible by the case $k = 11$ applied to $(n + 2d)(n + 4d) \cdots (n + 22d)$. Let $k = 24$. We get $(a_0, a_1, \ldots, a_{23}) = (5, 6, \ldots, 3, 7)$ or $(7, 3, \ldots, 6, 5)$ by applying the case $k = 23$ both to $n(n + d) \cdots (n + 22d)$ and $(n + d) \cdots (n + 23d)$. Further, the assertion for $25 \le k \le 28$ follows from $k = 24$.

Let $k \ge 29$. First we consider $k = 29$. We see from Lemmas 8, 6 and the case $k = 25$ that $29 \,|\, n + 4d$ or $29 \,|\, n + 5d$. Let $29 \,|\, n + 4d$. Then applying the case $k = 24$ to $(n + 5d)(n + 6d) \cdots (n + 28d)$, we get $(a_5, a_6, \ldots, a_{28}) = (5, 6, \ldots, 3, 7)$ or $(7, 3, \ldots, 6, 5)$. By observing $1 = \left(\frac{30}{29}\right) = \left(\frac{a_5a_6}{29}\right) = \left(\frac{1\cdot 2}{29}\right) = -1$, we may assume the second possibility. Then $a_1 = 1$, implying $1 = \left(\frac{a_2a_8}{29}\right) = \left(\frac{(-2)4}{29}\right) = -1$, a contradiction. Let $29 \,|\, n + 5d$. Now by considering $k = 23$ and $(n + 6d) \ldots (n + 28d)$, we get $(a_6, a_7, \ldots, a_{28}) \in \{(5, 6, \ldots, 26, 3), (6, 7, \ldots, 3, 7), (3, 26, \ldots, 6, 5), (7, 3, \ldots, 7, 6)\}$. Then we may restrict to the last possibility by considering the Legendre symbol mod 29 at the first two entries in the remaining possibilities. It follows that $a_3 = 1$, implying $1 = \left(\frac{a_3a_9}{29}\right) = \left(\frac{(-2)4}{29}\right) = -1$, a contradiction. This completes the proof for $k = 29$. We now proceed by induction. By Lemmas 8 and 6, the assertion follows for all primes k. Now Lemma 3 completes the proof of Theorem 4. ■

7. Proof of Theorem 1. Observe that for all tuples in (5) and (6), the product of the a_i's is not a square. Hence, by Theorem 4, we may assume that $101 \le k \le 109$. Assume (1). Then $\mathrm{ord}_p(a_0a_1 \cdots a_{k-1})$ is even for each prime p. Let $101 \le k \le 105$. Then $P(a_4a_5 \cdots a_{100}) \le 97$. Now the assertion follows from Theorem 4 by considering $(n + 4d) \cdots (n + 100d)$ and $k = 97$. Let $k = 106, 107$. Then $P(a_4a_5 \cdots a_{102}) \le 101$. We may suppose that $P(a_4a_5) = 101$ or $P(a_{101}a_{102}) = 101$, otherwise the assertion follows by the case $k = 99$ in Theorem 4. Let $P(a_4a_5) = 101$. Then $P(a_6 \cdots a_{102}) \le 97$ and the assertion follows by the case $k = 97$ in Theorem 4. This is also true when $P(a_{101}a_{102}) = 101$ since $P(a_4 \cdots a_{100}) \le 97$ in this case. Let $k = 108, 109$. Then $P(a_6 \cdots a_{102}) \le 101$. Thus either $P(a_6a_7) = 101$ or $P(a_{101}a_{102}) = 101$. Let $P(a_6a_7) = 101$. Then $P(a_8 \cdots a_{102}) \le 97$. We may assume that $97 \,|\, a_8a_9a_{10}a_{11}$ or $97 \,|\, a_{97} \cdots a_{101}a_{102}$. Let $97 \,|\, a_8a_9a_{10}a_{11}$. Then $P(a_{12}a_{13} \cdots a_{102}) \le 89$ and the assertion follows by the case $k = 91$ of Theorem 4. Let $97 \,|\, a_{97} \cdots a_{102}$. Then $P(a_8a_9 \cdots a_{96}) \le 89$ and the assertion follows from the case $k = 89$ of Theorem 4. When $P(a_{101}a_{102}) = 101$, we argue as above to get the assertion. ■

References

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

[BF05] N. Bruin and E. V. Flynn, *Towers of* 2*-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. 357 (2005), 4329–4347.

[Erd39] P. Erdős, *Note on the product of consecutive integers* (*II*), J. London Math. Soc. 14 (1939), 245–249.

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

[Eul80] L. Euler, Mém. Acad. Sci. St. Petersb. 8, 1817–1818 (1780), 3; Comm. Arith. Collectae II, 411–413.

[Lai04] S. Laishram, *Topics in Diophantine equations*, M.Sc. thesis, Mumbai Univ., 2004; online at http://www.math.tifr.res.in/~shanta/MScthesis.pdf.

[LS] S. Laishram and T. N. Shorey, *The equation* $n(n+d)\cdots(n+(k-1)d) = by^2$ *with* $\omega(d) \le 6$ *or* $d \le 10^{10}$, Acta Arith., to appear.

[Mor69] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[MS03] A. Mukhopadhyay and T. N. Shorey, *Almost squares in arithmetic progression* (*II*), Acta Arith. 110 (2003), 1–14.

[Obl50] R. Obláth, *Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reihe*, Publ. Math. Debrecen 1 (1950), 222–226.

[Rig39] O. Rigge, *Über ein diophantisches Problem*, in: C. R. 9$^{\text{ème}}$ Congrès des Mathématiciens Scandinaves (Helsingfors, 1938), Mercator, 1939, 155–160.

[Tij89] R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications, Kluwer, Dordrecht, 1989, 215–243.

Department of Mathematics
College of Science and Technology
Nihon University
Tokyo 101-8308, Japan
E-mail: hirata@math.cst.nihon-u.ac.jp

Mathematical Institute
Leiden University
2300 RA Leiden, The Netherlands
E-mail: tijdeman@math.leidenuniv.nl

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

Received on 2.12.2006
and in revised form on 13.4.2007 (5338)