SQUARES IN PRODUCTS IN ARITHMETIC PROGRESSION WITH AT MOST ONE TERM OMITTED AND COMMON DIFFERENCE A PRIME POWER

SHANTA LAISHRAM, T. N. SHOREY, AND SZABOLCS TENGELY

Abstract. It is shown that a product of $k-1$ terms out of $k \geq 7$ terms in arithmetic progression with common difference a prime power > 1 is not a square. In fact it is not of the form by^2 where the greatest prime factor of b is less than or equal to k. Also, we show that product of 11 or more terms in an arithmetic progression with common difference a prime power > 1 is not of the form by^2 where the greatest prime factor of b is less than or equal to $p_{\pi(k)+2}$.

1. Introduction

For an integer $x > 1$, we denote by $P(x)$ and $\omega(x)$ the greatest prime factor of x and the number of distinct prime divisors of x, respectively. Further we put $P(1) = 1$ and $\omega(1) = 0$. Let p_i be the $i-$th prime number. Let $k \geq 4, t \geq k-2$ and $\gamma_1 < \gamma_2 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Thus $t \in \{k, k-1, k-2\}, \gamma_t \geq k-3$ and $\gamma_i = i-1$ for $1 \leq i \leq t$ if $t = k$. We put $\psi = k - t$. Let b be a positive squarefree integer and we shall always assume, unless otherwise specified, that $P(b) \leq k$. We consider the equation

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

in positive integers n, d, k, b, y, t. It has been proved (see [SaSh03a] and [MuSh04a]) that (1.1) with $\psi = 1, k \geq 9$, $d \nmid n$, $P(b) < k$ and $\omega(d) = 1$ does not hold. Further it has been shown in [TSH06] that the assertion continues to be valid for $6 \leq k \leq 8$ provided $b = 1$. We show

Theorem 1. *Let $\psi = 1, k \geq 7$ and $d \nmid n$. Then (1.1) with $\omega(d) = 1$ does not hold.*

Thus the assumption $P(b) < k$ and $k \geq 9$ (in [SaSh03a] and [MuSh04a]) has been relaxed to $P(b) \leq k$ and $k \geq 7$, respectively, in Theorem 1. As an immediate consequence of Theorem 1, we see that (1.1) with $\psi = 0, k \geq 7$, $d \nmid n$, $P(b) \leq p_{\pi(k)+1}$ and $\omega(d) = 1$ is not possible. If $k \geq 11$, we relax the assumption $P(b) \leq p_{\pi(k)+1}$ to $P(b) \leq p_{\pi(k)+2}$ in the next result.

Theorem 2. *Let $\psi = 0, k \geq 11$ and $d \nmid n$. Assume that $P(b) \leq p_{\pi(k)+2}$ Then (1.1) with $\omega(d) = 1$ does not hold.*

For related results on (1.1), we refer to [LaSh07].

AMS Classification: Primary 11D61; Keywords: Diophantine equations, Arithmetic Progressions, Legendre symbol. Research of S. Tengely was supported in part by the Magyary Zoltán Higher Educational Public Foundation.

2. Notations and Preliminaries

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

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

with a_{γ_i} squarefree such that $P(a_{\gamma_i})\le \max(k-1,P(b))$. Thus (1.1) with b as the squarefree part of $a_{\gamma_1}\cdots a_{\gamma_t}$ is determined by the $t-$tuple $(a_{\gamma_1},\cdots,a_{\gamma_t})$. Further we write

$$b_i = a_{\gamma_i},\ y_i = x_{\gamma_i}.$$

Since $\gcd(n,d)=1$, we see from (2.1) that

$$(b_i,d)=(y_i,d)=1 \ \text{ for } 1\le i\le t. \tag{2.2}$$

Let

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

Lemma 2.1. ([LaSh07])
Equation (1.1) *with* $\omega(d)=1$ *and* $k\ge 9$ *implies that* $t-|R|\le 1$.

Lemma 2.2. *Let* $\psi=0, k\ge 4$ *and* $d\nmid n$. *Then* (1.1) *with* $\omega(d)=1$ *implies* $(n,d,k,b)=(75,23,4,6)$.

This is proved in [SaSh03a] and [MuSh03] unless $k=5, P(b)=5$ and then it is a particular case of a result of Tengely [Sz07].

Lemma 2.3. *(*[SaSh03a, Theorem 4] *and* [MuSh04a]*)*
Let $\psi=1, k\ge 9$ *and* $d\nmid n$. *Assume that* $P(b)<k$. *Then* (1.1) *with* $\omega(d)=1$ *does not hold.*

Lemma 2.4. ([LaSh07])
Let $\psi=2, k\ge 15$ *and* $d\nmid n$. *Then* (1.1) *with* $\omega(d)=1$ *does not hold.*

Lemma 2.5. *Let* $\psi=1, k=7$ *and* $d\nmid n$. *Then* $(a_0,a_1,\cdots,a_6)$ *is different from the ones given by the following tuples or their mirror images.*

$$\begin{aligned} k=7: &(1,2,3,-,5,6,7),(2,1,6,-,10,3,14),(2,1,14,3,10,-,6),\\ &(-,3,1,5,6,7,2),(3,1,5,6,7,2,-),(3,-,5,6,7,2,1),\\ &(1,5,6,7,2,-,10),(-,5,6,7,2,1,10),(5,6,7,2,1,10,-),\\ &(6,7,2,1,10,-,3),(10,3,14,1,2,5,-),\\ &(-,10,3,14,1,2,5),(5,2,1,14,3,10,-),(-,5,2,1,14,3,10). \end{aligned} \tag{2.3}$$

Further $(a_1,\cdots,a_6)$ *is different from* $(1,2,3,-,5,6),(2,1,6,-,10,3)$ *and their mirror images.*

The proof of Lemma 2.5 is given in Section 3.
The following result is contained in [BBGH06, Lemma 4.1].

Lemma 2.6. *There are no coprime positive integers n', d' satisfying the diophantine equations*

$$\prod(0,1,2,3)=by^2,\ b\in\{1,2,3,5,15\}$$
$$\prod(0,1,3,4)=by^2,\ b\in\{1,2,3,6,30\}$$

where $\prod(0,i,j,l)=n'(n'+id')(n'+jd')(n'+ld')$.

Lemma 2.7. *Equation* (1.1) *with* $\psi=1, k=7$ *is not possible if*

(i) $a_1=a_4=1, a_6=6$ *and either* $a_3=3$ *or* $a_2=2$
(ii) $a_1=a_6=1$ *and at least two of* $a_2=2, a_4=6, a_5=5$ *holds.*
(iii) $a_0=a_6=2$, $a_5=3$ *and either* $a_2=6$ *or* $a_4=1$
(iv) $a_0=a_5=1$ *and at least two of* $a_1=5, a_2=6$, $a_4=2$ *holds.*
(v) $a_3=a_6=1$, $a_1=6$ *and* $a_2=5$
(vi) $a_0=a_4=1$, $a_3=3$ *and* $a_6=2$
(vii) $a_0=a_5=1$ *and at least two of* $a_1=2, a_3=6, a_6=3$ *holds.*

Proof. The proof of Lemma 2.7 uses **MAGMA** to compute integral points on Quartic curves. For this we first make a Quartic curve and find a integral point on it. Then we compute all integral points on the curve by using **MAGMA** command *IntegralQuarticPoints* and we exclude them.

We illustrate this with one example and others are similar. Consider (ii). Then from $x_6^2-x_1^2=n+6d-(n+d)=5d$ and $\gcd(x_6-x_1,x_6+x_1)=1$, we get either

$$x_6-x_1=5, x_6+x_1=d \tag{2.4}$$

or

$$x_6-x_1=1, x_6+x_1=5d. \tag{2.5}$$

Assume (2.4). Then $d=2x_1+5$. This with $n+d=x_1^2$, we get

$$2x_2^2=n+2d=n+d+d=x_1^2+2x_1+5=(x_1+1)^2+4 \text{ if } a_2=2$$
$$6x_4^2=n+4d=n+d+3d=x_1^2+6x_1+15=(x_1+3)^2+6 \text{ if } a_4=6$$
$$5x_5^2=n+5d=n+d+4d=x_1^2+8x_1+20=(x_1+4)^2+4 \text{ if } a_5=5.$$

When $a_2=2, a_4=6$, by putting $X=x_1+1, Y=3(2x_2)(6x_4)$, we get the Quartic curve $Y^2=3(X^2+4)((X+2)^2+6)=3X^4+12X^3+42X^2+48X+120$ in positive integers X and Y with $X=x_1+1\geq 2$. Observing that $(X,Y)=(1,15)$ is an integral point on this curve, we obtain by **MAGMA** command

$$IntegralQuarticPoints([3,12,42,48,120],[1,15]);$$

that all integral points on the curve are given by

$$(X,Y)\in\{(1,\pm 15),(-2,\pm 12),(-14,\pm 300),(-29,\pm 1365).$$

Since none of the points (X,Y) satisfy $X\geq 2$, we exclude the case $a_2=2, a_4=6$. Further when $a_2=2, a_5=5$, by putting $X=x_1+1$ and $Y=10(2x_2)(5x_5)$, we get the curve $Y^2=10(X^2+4)((X+3)^2+4)=10X^4+60X^3+170X^2+240X+520$ for which an integral point is $(X,Y)=(-1,20)$ and all the integral points have $X\leq 1$ and it is excluded.

When $a_4 = 6, a_5 = 5$, by puting $X = x_1 + 3$ and $Y = 30(6x_4)(5x_5)$, we get the curve $Y^2 = 30(X^2+6)((X+1)^2+4) = 30X^4+60X^3+330X^2+360X+900$ for which $(X, Y) = (0, 30)$ is an integral point and all the integral points other than $(X, Y) = (11, 500)$ satisfy $X \leq 1$. Since $30|Y$ and $30 \nmid 500$, this case is also excluded. When (2.5) holds, we get $5d = 2x_1 + 1$ and this with $n + d = x_1^2$ implies

$$2(5x_2)^2 = 25(n + d) + 25d = 25x_1^2 + 10x_1 + 5 = (5x_1 + 1)^2 + 4 \text{ if } a_2 = 2$$
$$6(5x_4)^2 = 25(n + d) + 75d = 25x_1^2 + 30x_1 + 15 = (5x_1 + 3)^2 + 6 \text{ if } a_4 = 6$$
$$5(5x_5)^2 = 25(n + d) + 100d = 25x_1^2 + 40x_1 + 20 = (5x_1 + 4)^2 + 4 \text{ if } a_5 = 5.$$

As in the case (2.4), these gives rise to the same Quartic curves $Y^2 = 3X^4 + 12X^3 + 42X^2 + 48X + 120$; $Y^2 = 10X^4 + 60X^3 + 170X^2 + 240X + 520$ and $Y^2 = 30X^4 + 60X^3 + 330X^2 + 360X + 900$ when $a_2 = 2, a_3 = 6$; $a_2 = 2, a_5 = 5$ and $a_4 = 6, a_5 = 5$, respectively. This is not possible.

Similarly all the other cases are excluded. In the case (iii), we have $n = 2x_0^2$ and obtain either $d = 2x_0 + 3$ or $3d = 2x_0 + 1$. Then we use $2a_i x_i^2 = 2(n + id) = (2x_0)^2 + 2i(2x_0 + 3) = (2x_0 + i)^2 + 6i - i^2$ if $d = 2x_0 + 3$ and $2a_i(3x_i)^2 = 18(n + id) = (6x_0)^2 + 6i(2x_0 + 1) = (6x_0 + i)^2 + 6i - i^2$ if $3d = 2x_0 + 1$ to get Quartic equations. In the case (vi), we obtain the Quartic equation $Y^2 = 6X^4 + 36X^3 + 108X - 54 = 6(X^4 + 6X^3 + 18X - 9)$. For any integral point (X, Y) on this curve, we obtain $3|(X^4 + 6X^3 + 18X - 9)$ giving $3|X$. Then $\text{ord}_3(X^4 + 6X^3 + 18X - 9) = 2$ giving $\text{ord}_3(Y^2) = \text{ord}_3(6) + 2 = 3$, a contradiction. □

3. Proof of Lemma 2.5

For the proof of Lemma 2.5, we use the so-called elliptic Chabauty's method (see [NB02],[NB03]). Bruin's routines related to elliptic Chabauty's method are contained in MAGMA [MAGMA], so here we indicate the main steps only and a MAGMA routine which can be used to verify the computations. Note that in case of rank 0 elliptic curves one can compute the finitely many torsion points and check each of them if they correspond to any solutions. Therefore this case is not included in the routine. The input C is a hyperelliptic curve defined over a number field and p is a prime.

```
APsol:=function(C,p)
P1:=ProjectiveSpace(Rationals(),1);
E,toE:=EllipticCurve(C);
Em,EtoEm:=MinimalModel(E);
two:= MultiplicationByMMap(Em,2);
mu,tor:= DescentMaps(two);
S,AtoS:= SelmerGroup(two);
RB:=RankBound(Em: Isogeny:=two);
umap:=map<C->P1|[C.1,C.3]>;
U:=Expand(Inverse(toE*EtoEm)*umap);
if RB eq 0 then
   print "Rank 0 case";
   return true;
else
   success,G,mwmap:=PseudoMordellWeilGroup(Em: Isogeny:=two);
```

```
    if success then
      NC,VC,RC,CC:=Chabauty(mwmap,U,p);
      print "NC,#VC,RC:",NC,#VC,RC;
      PONTOK:={EvaluateByPowerSeries(U,mwmap(gp)): gp in VC};
      print "Saturated:",
        forall{pr: pr in PrimeDivisors(RC)|IsPSaturated(mwmap,pr)};
      return PONTOK;
    else return false;
    end if;
  end if;
  end function;
```

First consider the tuple $(6,7,2,1,10,-,3)$. Using that $n=6x_3^2-2x_2^2$ and $d=-2x_3^2+x_2^2$ we obtain the following system of equations

$$\begin{aligned} -x_3^2+3x_2^2 &= 3x_0^2,\\ -x_3^2+4x_2^2 &= 7x_1^2,\\ x_3^2-x_2^2 &= 5x_4^2,\\ 4x_3^2-6x_2^2 &= 3x_6^2. \end{aligned}$$

The first equation implies that x_3 is divisible by 3, that is there exists a $z\in\mathbb{Z}$ such that $x_3=3z$. By standard factorization argument we get that

$$(\sqrt{3}z+x_2)(3z+x_2)(12z^2-2x_2^2)=\delta\square,$$

where $\delta\in\{\pm 2+\sqrt{3},\pm 10+5\sqrt{3}\}$. Thus putting $X=z/x_2$ it is sufficient to find all points (X,Y) on the curves

$$C_\delta:\quad \delta(\sqrt{3}X+1)(3X+1)(12X^2-2)=Y^2, \tag{3.1}$$

for which $X\in\mathbb{Q}$ and $Y\in\mathbb{Q}(\sqrt{3})$. For all possible values of δ the point $(X,Y)=(-1/3,0)$ is on the curves, therefore we can transform them to elliptic curves. We note that $X=z/x_2=-1/3$ does not yield appropriate arithmetic progressions.

I. $\delta=2+\sqrt{3}$. In this case $C_{2+\sqrt{3}}$ is isomorphic to the elliptic curve

$$E_{2+\sqrt{3}}:\quad y^2=x^3+(-\sqrt{3}-1)x^2+(6\sqrt{3}-9)x+(11\sqrt{3}-19).$$

Using MAGMA we get that the rank of $E_{2+\sqrt{3}}$ is 0 and the only point on $C_{2+\sqrt{3}}$ for which $X\in\mathbb{Q}$ is $(X,Y)=(-1/3,0)$.

II. $\delta=-2+\sqrt{3}$. Applying elliptic Chabauty with $p=7$, we get that $z/x_2\in\{-1/2,-1/3,-33/74,0\}$. Among these values $z/x_2=-1/2$ gives $n=6,d=1$.

III. $\delta=10+5\sqrt{3}$. Applying again elliptic Chabauty with $p=23$, we get that $z/x_2\in\{1/2,-1/3\}$. Here $z/x_2=1/2$ corresponds to $n=6,d=1$.

IV. $\delta=-10+5\sqrt{3}$. The elliptic curve $E_{-10+5\sqrt{3}}$ is of rank 0 and the the only point on $C_{-10+5\sqrt{3}}$ for which $X\in\mathbb{Q}$ is $(X,Y)=(-1/3,0)$.

We proved that there is no arithmetic progression for which $(a_0,a_1,\dots,a_6)=(6,7,2,1,10,-,3)$ and $d\nmid n$.

Now consider the tuple $(1,5,6,7,2,-,10)$. The system of equation we use is

$$\begin{aligned} x_6^2 - 3x_1^2 &= -2x_0^2, \\ x_6^2 + 2x_1^2 &= 3x_2^2, \\ 4x_6^2 + 3x_1^2 &= 7x_3^2, \\ 3x_6^2 + x_1^2 &= x_4^2. \end{aligned}$$

We factor the first equation over $\mathbb{Q}(\sqrt{3})$ and the fourth over $\mathbb{Q}(\sqrt{-3})$. We obtain

$$\begin{aligned} x_6 + \sqrt{3}x_1 &= \delta_1\square, \\ \sqrt{-3}x_6 + x_1 &= \delta_2\square, \end{aligned}$$

where δ_1, δ_2 are from some finite sets (see e.g. [NSM98], pp. 50-51). The curves for which we apply elliptic Chabaty's method are

$$C_\delta : \quad 3\delta(X+\sqrt{3})(\sqrt{-3}X+1)(X^2+2) = Y^2,$$

defined over $Q(\alpha)$, where $\alpha^4 + 36 = 0$. It turnes out that there is no arithmetic progression with $(a_0, a_1, \ldots, a_6) = (1,5,6,7,2,-,10)$ and $d \nmid n$.

Note that in the remaining cases one can obtain the same system of equations for several tuples, these are

$$\begin{aligned} &(-,3,1,5,6,7,2) \text{ and } (3,1,5,6,7,2,-), \\ &(1,2,3,-,5,6) \text{ and } (2,1,6,-,10,3), \\ &(-,5,6,7,2,1,10) \text{ and } (5,6,7,2,1,10,-), \\ &(-,5,2,1,14,3,10) \text{ and } (-,10,3,14,1,2,5) \text{ and} \\ &(5,2,1,14,3,10,-) \text{ and } (10,3,14,1,2,5,-). \end{aligned}$$

In the table below we indicate the relevant quartic polynomials. These are as follows.

tuple	polynomial
$(-,3,1,5,6,7,2)$	$\delta_{A1}(X+\sqrt{-1})(2X+\sqrt{-1})(5X^2-1)$
$(-,5,2,1,14,3,10)$	$\delta_{A2}(X+\sqrt{-2})(2\sqrt{-2}X+1)(4X^2+3)$
$(-,5,6,7,2,1,10)$	$\delta_{A3}(X+\sqrt{-2})(2\sqrt{-2}X+1)(3X^2+1)$
$(1,2,3,-,5,6)$	$2\delta_{A4}(X+\sqrt{-1})(X+3\sqrt{-1})(5X^2-3)$
$(2,1,14,3,10,-,6)$	$\delta_{A5}(2X+\sqrt{-1})(3X+\sqrt{-1})(-3X^2+3)$
$(3,-,5,6,7,2,1)$	$5\delta_{A6}(2X+3\sqrt{-1})(X+\sqrt{-1})(12X^2-3)$

□

4. Proof of Theorem 1

Suppose that the assumptions of Theorem 1 are satisfied and assume (1.1) with $\omega(d) = 1$. Let $k \geq 15$. We may suppose that $P(b) = k$ otherwise it follows from (2.1) and Lemma 2.4. Then we delete the term divisible by k on the left hand side of (1.1) and the the assertion follows from Lemma 2.4. Thus it suffices to prove the assertion for $k \in \{7,8,11,13\}$ by Lemma 2.3. Therefore we always restrict to $k \in \{7,8,11,13\}$. In view of Lemma 2.1, we arrive at a contradiction by showing $t - |R| \geq 2$ when $k \in \{11,13\}$. Further Lemma 2.1 also implies that $p \nmid d$ for $p \leq k$ whenever $k \in \{11,13\}$.

For a prime $p \le k$ and $p \nmid d$, let i_p be such that $0 \le i_p < p$ and $p | n+i_p d$. For any subset $\mathcal{I} \subseteq [0,k) \cap \mathbb{Z}$ and primes p_1, p_2 with $p_i \le k$ and $p_i \nmid d$, $i=1,2$, we define

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

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

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

or

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

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

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

and

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

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

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

The equation (4.4) is called the mirror image of (1.1). The corresponding t-tuple $(a_{\gamma_1'}, a_{\gamma_2'}, \cdots, a_{\gamma_t'})$ is called the mirror image of $(a_{\gamma_1},\cdots,a_{\gamma_t})$.

4.1. **The case $k=7,8$.** We may assume that $k=7$ since the case $k=8$ follows from that of $k=7$.

In this subsection, we take $d \in \{2^\alpha, p^\alpha, 2p^\alpha\}$ where p is any odd prime and α is a positive integer. In fact, we prove

Lemma 4.1. *Let $\psi = 1, k=7$ and $d \nmid n$. Then (1.1) with $d \in \{2^\alpha, p^\alpha, 2p^\alpha\}$ does not hold.*

First we check that (1.1) does not hold for $d \le 23$ and $n+5d \le 324$. Thus we assume that either $d > 23$ or $n+5d > 324$. Hence $n+5d > 5\cdot 26 = 130$. Then (1.1) with $\psi = 0$, $k \ge 4$ and $\omega(d) = 1$ has no solution by Lemma 2.2. Let $d = 2$ or $d = 4$. Suppose $a_i = a_j$ with $i > j$. Then $x_i - x_j = r_1$ and $x_i + x_j = r_2$ with r_1, r_2 even and $\gcd(r_1,r_2) = 2$. Now from $n+id > 26i$, we get

$$i - j \ge \frac{a_i(x_i+x_j)}{2} \ge \frac{(a_i x_i^2)^{\frac{1}{2}} + (a_j a_j^2)^{\frac{1}{2}}}{2} > \frac{\sqrt{26(i+j)}}{2} > j,$$

a contradiction. Therefore $a_i \ne a_j$ whenever $i \ne j$ giving $|R| = k-1$. But $|\{a_i : P(a_i) \le 5\}| \le 4$ implying $|R| \le 4+1 < k-1$, a contradiction. Let $8|d$. Then $|\{a_i : P(a_i) \le 5\}| \le 1$ and $|\{j : a_j = a_i\}| \le 2$ for each $a_i \in R$ giving $|\{i : P(a_i) \le 5\}| \le 2$. This is a contradiction since $|\{i : P(a_i) \le 5\}| \ge 7-2 = 5$. Thus $d \ne 2^\alpha$. Let $t - |R| \ge 2$. Then we observe from [LaSh06a, Lemma] that $d_2 = d < 24$ and $n+5d < 324$. This is not possible.

Therefore $t-|R|\leq 1$ implying $|R|\geq k-2=5$. If $7|d$, then we get a contradiction since $7\nmid a_i$ for any i and $|\{a_i : P(a_i)\leq 5\}|\leq 4$ implying $|R|\leq 4<k-2$. If $3|d$ or $5|d$, then also we obtain a contradiction since $|\{a_i : P(a_i)\leq 5\}|\leq 2$ implying $|R|\leq 2+1<k-2$.

Thus $\gcd(p,d)=1$ for each prime $p\leq 7$. Therefore $5|n+i_5d$ and $7|n+i_7d$ with $0\leq i_5<5$ and $0\leq i_7<7$. By taking the mirror image (4.4) of (1.1), we may suppose that $0\leq i_7\leq 3$.

Let $p_1=5$, $p_2=7$ and $\mathcal{I}=\{\gamma_1,\gamma_2,\cdots,\gamma_6\}$. We observe that $P(a_i)\leq 3$ for $i\in\mathcal{M}\cup\mathcal{B}$. Since $\left(\frac{2}{5}\right)\neq\left(\frac{2}{7}\right)$ but $\left(\frac{3}{5}\right)=\left(\frac{3}{7}\right)$, we observe that $a_i\in\{2,6\}$ whenever $i\in\mathcal{M}$ and $a_i\in\{1,3\}$ whenever $i\in\mathcal{B}$.

We now define four sets

$$\mathcal{I}^k_{++}=\{i:0\leq i<k,\left(\frac{i-i_{p_1}}{p_1}\right)=\left(\frac{i-i_{p_2}}{p_2}\right)=1\},$$
$$\mathcal{I}^k_{--}=\{i:0\leq i<k,\left(\frac{i-i_{p_1}}{p_1}\right)=\left(\frac{i-i_{p_2}}{p_2}\right)=-1\},$$
$$\mathcal{I}^k_{+-}=\{i:0\leq i<k,\left(\frac{i-i_{p_1}}{p_1}\right)=1,\left(\frac{i-i_{p_2}}{p_2}\right)=-1\},$$
$$\mathcal{I}^k_{-+}=\{i:0\leq i<k,\left(\frac{i-i_{p_1}}{p_1}\right)=-1,\left(\frac{i-i_{p_2}}{p_2}\right)=1\}.$$

and let $\mathcal{I}_{++}=\mathcal{I}^k_{++}\cap\mathcal{I}$, $\mathcal{I}_{--}=\mathcal{I}^k_{--}\cap\mathcal{I}$, $\mathcal{I}_{+-}=\mathcal{I}^k_{+-}\cap\mathcal{I}$, $\mathcal{I}_{-+}=\mathcal{I}^k_{-+}\cap\mathcal{I}$. We observe here that $\mathcal{I}_1=\mathcal{I}_{++}\cup\mathcal{I}_{--}$ and $\mathcal{I}_2=\mathcal{I}_{+-}\cup\mathcal{I}_{-+}$. Since $a_i\in\{1,2,3,6\}$ for $i\in\mathcal{I}_1\cup\mathcal{I}_2$ and $\left(\frac{a_i}{p}\right)=\left(\frac{i-i_p}{p}\right)\left(\frac{d}{p}\right)$, we obtain four possibilities I,II,III and IV according as $\left(\frac{d}{5}\right)=\left(\frac{d}{7}\right)=1$; $\left(\frac{d}{5}\right)=\left(\frac{d}{7}\right)=-1$; $\left(\frac{d}{5}\right)=1,\left(\frac{d}{7}\right)=-1$; $\left(\frac{d}{5}\right)=-1,\left(\frac{d}{7}\right)=1$, respectively.

	$\{a_i : i\in\mathcal{I}_{++}\}$	$\{a_i : i\in\mathcal{I}_{--}\}$	$\{a_i : i\in\mathcal{I}_{+-}\}$	$\{a_i : i\in\mathcal{I}_{-+}\}$
I	$\{1\}$	$\{3\}$	$\{6\}$	$\{2\}$
II	$\{3\}$	$\{1\}$	$\{2\}$	$\{6\}$
III	$\{2\}$	$\{6\}$	$\{3\}$	$\{1\}$
IV	$\{6\}$	$\{2\}$	$\{1\}$	$\{3\}$

In the case I, we have $\left(\frac{a_i}{p}\right)=\left(\frac{i-i_p}{p}\right)$ for $p\in\{5,7\}$ which together with $\left(\frac{a_i}{5}\right)=1$ for $a_i\in\{1,6\}$, $\left(\frac{a_i}{5}\right)=-1$ for $a_i\in\{2,3\}$, $\left(\frac{a_i}{7}\right)=1$ for $a_i\in\{1,2\}$ and $\left(\frac{a_i}{7}\right)=-1$ for $a_i\in\{3,6\}$ implies the assertion. The assertion for the cases II,III and IV follows similarly. For simplicity, we write $\mathcal{A}_7=(a_0,a_1,a_2,a_3,a_4,a_5,a_6)$.

For each possibility $0\leq i_5<5$ and $0\leq i_7\leq 3$, we compute $\mathcal{I}^k_{++},\mathcal{I}^k_{--},\mathcal{I}^k_{+-},\mathcal{I}^k_{+-}$ and restrict to those pairs (i_5,i_7) for which $\max(|\mathcal{I}^k_1|,|\mathcal{I}^k_2|)\leq 4$. Then we check for the possibilities I,II,III or IV.

Suppose $d=2p^\alpha$. Then $b_i\in\{1,3\}$ whenever $P(b_i)\leq 3$. If $i_5\neq 0,1$, then $|R|\leq 2+2=4$ giving $t-|R|\geq 7-1-4=2$, a contradiction. Thus $i_5\in\{0,1\}$. Further $\mathcal{M}=\emptyset$ and $a_i\in\{1,3\}$ for $i\in\mathcal{B}$. Therefore either $|\mathcal{I}^k_1|\leq 1$ or $|\mathcal{I}^k_1|\leq 2$. We find that this is the case only when $(i_5,i_7)\in\{(0,1),(1,2)$. Let $(i_5,i_7)=(0,1)$. We get $\mathcal{I}^k_{++}=\mathcal{I}^k_{--}=\emptyset$, $\mathcal{I}^k_{+-}=\{4,6\}$ and $\mathcal{I}^k_{-+}=\{2,3\}$. It suffices to consider the cases III and IV since $b_i\in\{1,3\}$ whenever $P(b_i)\leq 3$. Suppose III holds. Then by modulo 3, we obtain $4\notin\mathcal{I}$, $a_6=3$ and $a_2=a_3=1$. By modulo 3 again, we get $a_1\notin\{1,7,3\}$ which is not possible since $5\nmid a_1$. Suppose IV holds. Then by modulo 3, we obtain $2\notin\mathcal{I}$, $a_4=a_6=1$ and $a_3=3$. We now get $a_1\in\{1,7\}$

and by $t-|R|\leq 1$, we get $a_1=7$. This is not possible since $-1=\left(\frac{a_1a_4}{5}\right)=\left(\frac{(1-0)(4-0)}{5}\right)=1$. Similarly $(i_5,i_7)=(1,2)$ is excluded. Hence $d=p^\alpha$ from now on.

Let $(i_5,i_7)=(0,0)$. We obtain $\mathcal{I}^k_{++}=\{1,4\},\mathcal{I}^k_{--}=\{3\}$, $\mathcal{I}^k_{+-}=\{6\}$ and $\mathcal{I}^k_{-+}=\{2\}$. We may assume that $1\in\mathcal{I}$ otherwise $P(a_2a_3a_4a_5a_6)\leq 5$ and this is excluded by Lemma 2.2 with $k=5$. Further $i\notin\mathcal{I}$ for exactly one of $i\in\{2,3,4\}$ otherwise $P(a_1a_2a_3a_4)\leq 3$ and this is not possible by Lemma 2.2 with $k=4$ since $d>23$. Consider the possibilities II and IV. By modulo 3, we obtain $2\notin\mathcal{I}$, $3|a_1a_4$ and $a_3a_6=2$. This is not possible by modulo 3 since $-1=\left(\frac{a_3a_6}{3}\right)=\left(\frac{(3-1)(6-1)}{3}\right)=1$, a contradiction. Suppose I holds. Then $a_1=1$ and $a_6=6$. If $4\in\mathcal{I}$, then $a_1=a_4=1$ and at least one of $a_3=3,a_2=2$ holds and this is excluded by Lemma 2.7 (i). Assume that $4\notin\mathcal{I}$. Then $a_1=1,a_2=2,a_3=3,a_6=6$ giving $a_5=5$ by modulo 2 and 3. Thus we have $(a_1,\cdots,a_5,a_6)=(1,2,3,-,5,6)$. This is not possible by Lemma 2.5. Suppose III holds. Then $4\notin\mathcal{I}$, $a_1=2,a_2=1,a_3=6,a_6=3$ giving $a_5=10$ by modulo 2 and 3. Thus $(a_1,\cdots,a_5,a_6)=(2,1,6,-,10,3)$ which is also excluded by Lemma 2.5.

Let $(i_5,i_7)=(0,1)$. We obtain $\mathcal{I}^k_{++}=\mathcal{I}^k_{--}=\emptyset$, $\mathcal{I}^k_{+-}=\{4,6\}$ and $\mathcal{I}^k_{-+}=\{2,3\}$. The possibility I is excluded by parity and modulo 3. The possibility II implies that $3\notin\mathcal{I}$, $a_4=a_6=2$ and $a_2=3$. This is not possible by modulo 3. Suppose III holds. Then $a_2=a_3=1$ and either $4\notin\mathcal{I},a_6=3$ or $6\notin\mathcal{I},a_4=3$. By modulo 3, we obtain $4\notin\mathcal{I},a_6=3$ and $\left(\frac{a_5}{3}\right)=\left(\frac{a_2}{3}\right)=1$. This gives $a_5\in\{1,10\}$ which together with $t-|R|\leq 1$ implies $a_5=10$. But this is not possible by Lemma 2.6 with $n'=n+2d,d'=d$ and $(i,j,l)=(1,3,4)$. Hence III is excluded. Suppose IV holds. Then $a_4=a_6=1$ and $2\notin\mathcal{I},a_3=3$ by modulo 3. By modulo 3, we get $a_5\in\{2,5\}$ and we may take $a_5=5$ otherwise we get a contradiction from $d>23$ and Lemma 2.2 with $k=4$ applied to $(n+3d)(n+4d)(n+5d)(n+6d)$. This is again not possible by Lemma 2.6 with $n'=n+3d,d'=d$ and $(i,j,l)=(1,2,3)$.

Let $(i_5,i_7)=(0,3)$. We obtain $\mathcal{I}^k_{++}=\{4\},\mathcal{I}^k_{--}=\{2\}$, $\mathcal{I}^k_{+-}=\{1,6\}$ and $\mathcal{I}^k_{-+}=\emptyset$. By modulo 3, we observe that the possibilities I and III are excluded. Suppose II happens. Then $a_2=1,a_4=3$ and either $a_6=2,1\notin\mathcal{I}$ or $a_1=2,6\notin\mathcal{I}$. If $a_6=2,1\notin\mathcal{I}$, then $a_5\in\{1,5\}$ which gives $a_5=1$ by modulo 3. This is not possible by modulo 7 since $-1=\left(\frac{a_4a_5}{7}\right)=\left(\frac{(4-3)(5-3)}{7}\right)=1$. Thus $a_1=2,6\notin\mathcal{I}$. Then $a_0=5,a_5=10,a_3=14$ by modulo 3 giving $(a_0,a_1,\cdots,a_5,a_6)=(5,2,1,14,3,10,-)$. Suppose IV happens. Let $1,6\in\mathcal{I}$. Then $a_1=a_6=1$ and either $a_2=2$ or $a_4=6$. By Lemma 2.7 (ii), we may assume that either $2\notin\mathcal{I}$ or $4\notin\mathcal{I}$. If $2\notin\mathcal{I}$, then $a_4=6$, $a_3=7$ and $a_5=5$ which is excluded by Lemma 2.7 (ii). Thus $4\notin\mathcal{I}$, $a_2=2$ and $a_5=5$ since $3\nmid a_5$. This is also excluded by Lemma 2.7 (ii). Therefore $a_2=2,a_4=6$ and either $6\notin\mathcal{I},a_1=1$ or $1\notin\mathcal{I},a_6=1$. Now $7|a_3$ otherwise $P(a_1a_2\cdots a_5)\leq 5$ if $1\in\mathcal{I}$ or $P(a_2a_3\cdots a_6)\leq 5$ if $6\in\mathcal{I}$ and this is excluded by Lemma 2.2 with $k=5$. Further by modulo 3, we get $a_3=7$, $a_0=10$ and $a_5=5$. Hence we obtain $\mathcal{A}_7=(10,-,2,7,6,5,1)$ or $\mathcal{A}_7=(10,1,2,7,6,5,-)$.

Let $(i_5,i_7)=(1,0)$. We obtain $\mathcal{I}^k_{++}=\{2\},\mathcal{I}^k_{--}=\{3\}$, $\mathcal{I}^k_{+-}=\{5\}$ and $\mathcal{I}^k_{-+}=\{4\}$. We consider the possibility I. By parity argument, we have either $5\notin\mathcal{I}$ or $4\notin\mathcal{I}$. Again by modulo 3, either $3\notin\mathcal{I}$ or $5\notin\mathcal{I}$. Thus $5\notin\mathcal{I}$ giving $a_2=1,a_3=3,a_4=2$. Now $5|a_1$ otherwise we get a contradiction from $P(a_1a_2a_3a_4)\leq 3$, Lemma 2.2 with $k=4$ and $d>23$. Hence $a_1=5$. This is a again a contradiction since $-1=\left(\frac{a_1a_2}{7}\right)=\left(\frac{(1-0)(2-0)}{7}\right)=1$. Thus the possibility I is excluded. If the possibility III holds, then $3\notin\mathcal{I}$, $a_2=2,a_5=3,a_4=1$

giving $a_1 \in \{1,5\}$ and $a_6 = 5$. By modulo 3, we get $a_1 = 1$. But this is not possible by Lemma 2.6 with $n' = n+2d, d' = d$ and $(i,j,l) = (1,3,4)$. Similarly, the possibilities II and IV are also excluded. If II holds, then $4 \notin \mathcal{I}, a_2 = 3, a_3 = 1, a_5 = 2$. Now $a_6 \in \{1,5\}$ and further by modulo 3, we get $a_6 = 1$. This is not possible by Lemma 2.6 with $n' = n+2d, d' = d$ and $(i,j,l) = (1,3,4)$. If IV holds, then $2 \notin \mathcal{I}$, $a_3 = 2$, $a_5 = 1, a_4 = 3$. Then $a_6 \in \{1,5\}$ giving $a_6 = 5$ by modulo 3. This is not possible modulo 7.

Let $(i_5, i_7) = (1,1)$. We obtain $\mathcal{I}^k_{++} = \{2,5\}, \mathcal{I}^k_{--} = \{4\}$, $\mathcal{I}^k_{+-} = \{0\}$ and $\mathcal{I}^k_{-+} = \{3\}$. We consider the possibilities III and IV. By parity, we obtain $5 \notin \mathcal{I}$. But then we get a contradiction modulo 3 since $a_4 = 6, a_0 = 3$ if III holds and $a_2 = 6, a_3 = 3$ if IV holds are not possible. Next we consider the possibility I. Then $0 \notin \mathcal{I}$ by modulo 2 and 3 and we get $P(a_2 a_3 \cdots a_6) \le 5$ and this is excluded by Lemma 2.2 with $k = 5$. Let II holds. Then $3 \notin \mathcal{I}$ by modulo 2 and 3 and $a_2 = a_5 = 3, a_4 = 1, a_0 = 2$. Further $a_6 \in \{5, 10\}$ which together with modulo 3 gives $a_6 = 5$. Now we get a contradiction modulo 7 from $a_5 = 3, a_6 = 5$.

Let $(i_5, i_7) = (3,1)$. We obtain $\mathcal{I}^k_{++} = \{2\}, \mathcal{I}^k_{--} = \{0,6\}$, $\mathcal{I}^k_{+-} = \{4\}$ and $\mathcal{I}^k_{-+} = \{5\}$. We may assume that $i \notin \mathcal{I}$ for exactly one of $i \in \{0,2,4,6\}$ otherwise n is even, $P(a_0 a_2 a_4 a_6) \le 3$ and this is excluded by $k = 4$ of Lemma 2.2 applied to $\frac{n}{2}(\frac{n}{2}+d)(\frac{n}{2}+2d)(\frac{n}{2}+3d)$. We consider the possibilities I and III. By modulo 3, we get $4 \notin \mathcal{I}$, $a_0 = a_6$, $3|a_0$ and $a_2 a_5 = 2$. This is not possible by modulo 3. Next we consider the possibility II. Then $4 \notin \mathcal{I}$ by parity argument. Further $a_0 = a_6 = 1$, $a_2 = 3, a_5 = 6$. This is not possible since $8|x_6^2 - x_0^2 = n+6d-n = 6d$ and d is odd. Finally we consider the possibility IV. If $2 \notin \mathcal{I}$ or $4 \notin \mathcal{I}$, then $a_0 = a_6 = 2, a_5 = 3$ and one of $a_2 = 6$ or $a_4 = 1$. This is excluded by Lemma 2.7 (iii). Thus $a_2 = 6, a_4 = 1, a_5 = 3$ and either $a_0 = 2, 6 \notin \mathcal{I}$ or $a_6 = 2, 0 \notin \mathcal{I}$. Then $a_1 = 7, a_3 = 5$ by parity and modulo 3. Hence $\mathcal{A}_7 = (2,7,6,5,1,3,-)$ or $\mathcal{A}_7 = (-,7,6,5,1,3,2)$.

All the other pairs are excluded similarly. For $(i_5, i_7) = (0,2)$, we obtain either $\mathcal{A}_7 = (1,2,3,-,5,6)$ or $(5,6,7,2,1,10,-)$ or $(10,3,14,1,2,5,-)$ which are excluded by Lemma 2.5. For $(i_5, i_7) = (1,3)$, we obtain $\mathcal{A}_7 = (1,5,6,7,2,-,10)$, $(-,5,6,7,2,1,10)$ or $(-,10,3,14,1,2,5)$ which is not possible by Lemma 2.5 or $a_0 = a_5 = 1$ and at least two of $a_1 = 5, a_2 = 6$, $a_4 = 2$ holds which is again excluded by Lemma 2.7 (iv). For $(i_5, i_7) = (2,0)$, we obtain $\mathcal{A}_7 = (14,3,10,-,6,1,2), (7,6,5,-,3,2,1)$ or $a_3 = a_6 = 1, a_0 = 7, a_1 = 6, a_2 = 5$, $a_4 = 3$ or $a_5 = 2$. These are Lemma 2.7 (v). For $(i_5, i_7) = (2,1)$, we obtain $a_0 = a_4 = 1, a_3 = 3, a_6 = 2$ which is not possible by Lemma 2.7 (vi). For $(i_5, i_7) = (4,1)$, we obtain $\mathcal{A}_7 = (6,7,2,1,10,-,3)$ which is also excluded. For $(i_5, i_7) = (4,2)$, we obtain $\mathcal{A}_7 = (2,1,14,3,10,-,6), (1,2,7,6,5,-,3), (-,2,7,6,5,1,3)$ or $a_0 = a_5 = 1$ and at least two of $a_1 = 2, a_3 = 6, a_6 = 3$ holds. The previous possibility is excluded by Lemma 2.5 and the latter by Lemma 2.7 (vii).

4.2. **The case $k = 11$.** We may assume that $11|a_i$ for some i but $11 \nmid a_0 a_1 a_2 a_3 a_7 a_8 a_9 a_{10}$ otherwise the assertion follows from Lemma 4.1. Further we may also suppose that $i \in \{4,5,6\}$ whenever $i \notin \mathcal{I}$ otherwise the assertion follows from Lemma 4.1.

Let $p_1 = 5$, $p_2 = 11$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. We observe that $P(a_i) \le 7$ for $i \in \mathcal{M} \cup \mathcal{B}$. Since $\left(\frac{3}{5}\right) \ne \left(\frac{3}{11}\right)$ but $\left(\frac{q}{5}\right) = \left(\frac{q}{11}\right)$ for a prime $q < k$ other than $3, 5, 11$, we observe that $3|a_i$ whenever $i \in \mathcal{M}$. Since $\sigma_3 \le 4$ and $|\mathcal{I}| = k-1$, we obtain from (4.3) that $|\mathcal{M}^k| \le 5$ and $3|a_i$ for at least $|\mathcal{M}^k| - 1$ i's with $i \in \mathcal{M}^k$. Further $a_i \in \{1,2,7,14\}$ for $i \in \mathcal{B}$ giving $|\mathcal{B}| \le 5$ otherwise $t - |R| \ge 2$. Hence $|\mathcal{B}^k| \le 6$ by (4.3).

By taking the mirror image (4.4) of (1.1), we may suppose that $4 \le i_{11} \le 5$. For each possibility $0 \le i_5 < 5$ and $4 \le i_{11} \le 5$, we compute $|\mathcal{I}^k_1|, |\mathcal{I}^k_2|$ and restrict to those pairs

(i_5, i_{11}) for which $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 6$. Further we restrict to those pairs (i_5, i_{11}) for which either

$$3|a_i \text{ for at least } |\mathcal{I}_1^k| - 1 \text{ elements } i \in \mathcal{I}_1^k \tag{4.5}$$

or

$$3|a_i \text{ for at least } |\mathcal{I}_2^k| - 1 \text{ elements } i \in \mathcal{I}_2^k. \tag{4.6}$$

We find that exactly one of (4.5) or (4.6) happens. We have $\mathcal{M}^k = \mathcal{I}_1^k, \mathcal{B}^k = \mathcal{I}_2^k$ when (4.5) holds and $\mathcal{M}^k = \mathcal{I}_2^k, \mathcal{B}^k = \mathcal{I}_1^k$ when (4.6) holds. If $3|a_i$ for exactly $|\mathcal{M}^k|-1$ elements $i \in \mathcal{M}^k$, then $\mathcal{B} = \mathcal{B}^k$ and we restrict to such pairs (i_5, i_{11}) for which there are at most 3 elements $i \in \mathcal{B}^k$ with $P(a_i) \leq 2$ otherwise $t - |R| \geq 2$. Now all the pairs (i_5, i_{11}) are excluded other than

$$(0,4), (1,5), (4,5). \tag{4.7}$$

For these pairs, we find that $|\mathcal{B}^k| \geq 5$. Hence we may suppose that $7|a_i$ for some $i \in \mathcal{B}$ otherwise $a_i \in \{1,2\}$ for $i \in \mathcal{B}$ which together with $|\mathcal{B}| \geq 4$ gives $t - |R| \geq 2$. Further if $|\mathcal{B}^k| = 6$, then we may assume that $7|a_i, 7|a_{i+7}$ for some $0 \leq i \leq 3$.

Let $(i_5, i_{11}) = (0,4)$. Then $\mathcal{M}^k = \{3,9\}$ and $\mathcal{B}^k = \{1,2,6,7,8\}$ giving $i_3 = 0$. If $7|a_6a_7$, then $|\mathcal{B}| = |\mathcal{B}^k| - 1$ and $a_i \in \{3,6\}$ for $i \in \mathcal{M} = \mathcal{M}^k$ but $\left(\frac{a_3a_9}{7}\right) = \left(\frac{(3-i_7)(9-i_7)}{7}\right) = -1$ for $i_7 = 6, 7$, a contradiction. If $7|a_2$, then $a_i \in \{5, 10\}$ for $i \in \{5, 10\} \subseteq \mathcal{I}$ but $\left(\frac{a_5a_{10}}{7}\right) = \left(\frac{(5-2)(10-2)}{7}\right) = -1$, a contradiction again. Thus $7|a_1a_8$ and $a_i \in \{1,2\}$ for $\{2,6,7\} \cap \mathcal{B}^k$. From $\left(\frac{a_i}{7}\right) = \left(\frac{i-1}{7}\right)\left(\frac{d}{7}\right)$, $\left(\frac{6-1}{7}\right) = \left(\frac{7-1}{7}\right) = -1$ and $\left(\frac{2-1}{7}\right) = 1$, we find that $2 \notin \mathcal{I}$. This is not possible.

Let $(i_5, i_{11}) = (1,5)$. Then $\mathcal{M}^k = \{4, 10\}$ and $\mathcal{B}^k = \{0,2,3,7,8,9\}$ giving $i_3 = 1$. Thus $\mathcal{M} = \mathcal{M}^k$, $a_i \in \{3,6\}$ for $i \in \mathcal{M}$ and $|\mathcal{B}| = |\mathcal{B}^k| - 1$, $a_i \in \{1,2,7,14\}$ for $i \in \mathcal{B}$. Further we have either $7|a_0a_7$ or $7|a_2a_9$. Taking modulo $\left(\frac{a_i}{7}\right)$ for $i \in \{4, 10, 0, 2, 3, 7, 8, 9\}$, we find that $7|a_2a_9$ and $3 \notin \mathcal{B}$. This is not possible.

Let $(i_5, i_{11}) = (4,5)$. Then $\mathcal{M}^k = \{0,6\}$ and $\mathcal{B}^k = \{1,2,3,7,8,10\}$ giving $\mathcal{M} = \mathcal{M}^k$ and $i_3 = 0$. Further $7|a_1a_8$ or $7|a_3a_{10}$. Taking modulo $\left(\frac{a_i}{7}\right)$ for $i \in \mathcal{M} \cup \mathcal{B}^k$, we find that $7|a_1a_8$ and $\mathcal{B} = \mathcal{B}^k \setminus \{7\}$. This is not possible since $7 \in \mathcal{I}$.

4.3. **The case $k = 13$.** We may assume that $13 \nmid a_0a_1a_2a_{10}a_{11}a_{12}$ otherwise the assertion follows from Theorem 1 with $k = 11$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q = 2, 3, 7$, we observe that for $5|a_i$ for $i \in \mathcal{M}$ and $P(a_i) \leq 7$, $5 \nmid a_i$ for $i \in \mathcal{B}$. Since $\sigma_5 \leq 3$, we obtain $|\mathcal{M}^k| \leq 4$ and $5|a_i$ for at least $|\mathcal{M}^k| - 1$ i's with $i \in \mathcal{M}^k$.

By taking the mirror image (4.4) of (1.1), we may suppose that $3 \leq i_{13} \leq 6$ and $0 \leq i_{11} \leq 10$. We may suppose that $i_{13} \geq 4, 5$ if $i_{11} = 0, 1$, respectively and $\max(i_{11}, i_{13}) \geq 6$ if $i_{11} \geq 2$ otherwise the assertion follows from Lemma 4.1.

Since $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 5$ and $|\mathcal{M}^k| \leq 4$, we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 4$ and further $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11}, i_{13}) for which $5|a_i$ for at least $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$. If $5|a_i$ for exactly $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$, then $\mathcal{B} = \mathcal{B}^k$ and hence we may assume that $|\mathcal{B}| = |\mathcal{B}^k| \leq 7$ otherwise there are at least 6 elements $i \in \mathcal{B}$ for which $a_i \in \{1,2,3,6\}$ giving $t - |R| \geq 2$. Therefore we now exclude those pairs (i_{11}, i_{13}) for which

$5|a_i$ for exactly $|\mathcal{M}^k|-1$ elements $i\in\mathcal{M}^k$ and $|\mathcal{B}^k|>7$. We find that all the pairs (i_{11},i_{13}) are excluded other than

$$(1,3),(2,4),(3,5),(4,2),(5,3),(6,4). \tag{4.8}$$

From $i_{13}\geq 5$ if $i_{11}=1$ and $\max(i_{11},i_{13})\geq 6$ if $i_{11}\geq 2$, we find that all these pairs are excluded other than $(6,4)$.

Let $(i_{11},i_{13})=(6,4)$. Then $\mathcal{M}^k=\{0,2,7,12\}$ and $\mathcal{B}^k=\{1,3,5,8,9,10,11\}$ giving $i_5=1$, $\mathcal{M}=\{2,7,12\}$ and $0\notin\mathcal{I}$. This is excluded by applying Lemma 4.1 to $\prod_{i=0}^{5}(n+d+2i)$. □

5. Proof of Theorem 2

By Lemma 2.2, we may suppose that $P(b)>k$. If $P(b)=p_{\pi(k)+1}$ or $P(b)=p_{\pi(k)+2}$ with $p_{\pi(k)+1}\nmid b$, then the assertion follows from Theorem 1. Thus we may suppose that $P(b)=p_{\pi(k)+2}$ and $p_{\pi(k)+1}|b$. Then we delete the terms divisible by $p_{\pi(k)+1},p_{\pi(k)+2}$ on the left hand side of (1.1) and the assertion for $k\geq 15$ follows from Lemma 2.4. Thus $11\leq k\leq 14$ and it suffices to prove the assertion for $k=11$ and $k=13$. After removing the i's for which $p|a_i$ with $p\in\{13,17\}$ when $k=11$ and $p|a_i$ with $p\in\{17,19\}$ when $k=13$, we observe that from Lemma 2.1 that $k-|R|\leq 1$ and $p\nmid d$ for each $p\leq k$.

5.1. **The case $k=11$.** Let $p_1=11$, $p_2=13$ and $\mathcal{I}=\{0,1,2,\cdots,10\}$. Since $\left(\frac{5}{11}\right)\neq\left(\frac{5}{13}\right)$, $\left(\frac{17}{11}\right)\neq\left(\frac{17}{13}\right)$ but $\left(\frac{q}{11}\right)=\left(\frac{q}{13}\right)$ for $q=2,3,7$, we observe that either $5|a_i$ or $17|a_i$ for $i\in\mathcal{M}$ and either $5\cdot 17|a_i$ or $P(a_i)\leq 7$ for $i\in\mathcal{B}$. Since $\sigma_5\leq 3$, we obtain $|\mathcal{M}|\leq 4$.

By taking the mirror image (4.4) of (1.1), we may suppose that $0\leq i_{13}\leq 5$ and $0\leq i_{11}\leq 10$. If both i_{11},i_{13} are odd, then we may suppose that i_{17} is even otherwise we get a contradiction from Lemma 4.1 applied to $\prod_{i=0}^{5}a_{n+i(2d)}$. Also we may suppose that $\max(i_{11},i_{13})\geq 4$ otherwise we get a contradiction from Lemma 4.1 applied to $\prod_{i=0}^{6}a_{n+4d+id}$. Further from Lemma 4.1, we may assume $i_{17}>4$ if $\max(i_{11},i_{13})=4$.

Since $\max(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\geq 5$ and $|\mathcal{M}^k|\leq 4$, we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\leq 4$ and further $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11},i_{13}) for which either $5|a_i$ or $17|a_i$ whenever $i\in\mathcal{M}$. Let $\mathcal{B}'=\mathcal{B}\setminus\{i:5\cdot 17|a_i\}$. If $|\mathcal{B}'|\geq 8$, then there are at least 6 elements $i\in\mathcal{B}'$ such that $P(a_i)\leq 3$ giving $k-|R|\geq 2$. Thus we restrict to those pairs for which $|\mathcal{B}'|\leq 7$. Further we observe that $7|a_i$ and $7|a_{i+7}$ for some $i,i+7\in\mathcal{B}'$ if $|\mathcal{B}'|=7$.

Let $(i_{11},i_{13})=(2,4)$. Then $\mathcal{M}^k=\{1,6,8\}$ and $\mathcal{B}^k=\{0,3,5,7,9,10\}$ giving $i_5=1$, $17|a_8$ and $P(a_i)\leq 7$ for $i\in\mathcal{B}$. For each possibility $i_7\in\{0,3,4,5\}$, and $i_{17}=8$, we take $p_1=7,p_2=17$, $\mathcal{I}=\mathcal{B}^k$ and compute $\mathcal{I}_1$ and $\mathcal{I}_2$. Since $\left(\frac{p}{7}\right)=\left(\frac{p}{17}\right)$ for $p\in\{2,3\}$, we should have either $\mathcal{I}_1=\emptyset$ or $\mathcal{I}_2=\emptyset$. We find that $\min(|\mathcal{I}_1|,|\mathcal{I}_2|)>0$ for each possibility $i_7\in\{0,3,4,5\}$. Hence $(i_{11},i_{13})=(2,4)$ is excluded. Similarly all pairs (i_{11},i_{13}) are excluded except $(i_{11},i_{13})\in\{(4,2),(6,4)\}$. When $(i_{11},i_{13})=(3,5)$, we get $\mathcal{M}^k=\{2,7,9\}$ giving $5|a_2a_7$, $17|a_9$ and hence it is excluded. When $(i_{11},i_{13})=(1,4)$, we obtain $\mathcal{M}^k=\{5,9\}$ and $\mathcal{B}^k=\{0,2,3,6,7,8,10\}$ giving either $5|a_5,17|a_9$ or $17|a_5,5|a_9$. Also $i_7\in\{0,3\}$. Thus we have $(i_7,i_{17})\in\{(0,5),(0,9),(3,5),(3,9)\}$ and apply the procedure for each of these possibilities.

Let $(i_{11},i_{13})=(6,4)$. Then $\mathcal{M}^k=\{0,2,7\}$ and $\mathcal{B}^k=\{1,3,5,8,9,10\}$ giving $i_5=2$, $17|a_0$ and $P(a_i)\leq 7$ for $i\in\mathcal{B}$. For each possibility $i_7\in\{1,3,4,5\}$, and $i_{17}=0$, we take $p_1=7,p_2=17$ and $\mathcal{I}=\mathcal{B}^k$. Since $\left(\frac{p}{7}\right)=\left(\frac{p}{17}\right)$ for $p\in\{2,3\}$, we observe that either $\mathcal{I}_1=\emptyset$ or $\mathcal{I}_2=\emptyset$. We find that this happens only when $i_7=3$ where we get $\mathcal{I}_1=\emptyset$ and $\mathcal{I}_2=\{1,5,8,9\}$. By taking modulo 7, we get $a_i\in\{1,2\}$ for $i\in\{1,8,9\}$ and $a_5\in\{3,6\}$. Further by modulo 5,

we obtain $a_1=a_8=1, a_9=2, a_5=3$, $a_14, a_{10}=7$ and this is excluded by Runge's method. When $(i_{11},i_{13})=(4,2)$, we get $\mathcal{M}^k=\{0,5,10\}$ and $\mathcal{B}^k=\{1,3,6,7,8,9\}$ giving $5|a_0a_5a_{10}$ and $i_{17}\in\{5,10\}$. Here we obtain $i_{17}=10, i_7=3$ where $\mathcal{I}_1=\emptyset$ and $\mathcal{I}_2=\{1,6,7,8,9\}$. This is not possible by Lemma 2.2 with $k=4$ applied to $(n+6d)(n+6d+d)(n+6d+2d)(n+6d+3d)$.

5.2. **The case** $k=13$**.** Let $p_1=11$, $p_2=13$ and $\mathcal{I}=\{0,1,2,\cdots,12\}$. Since $\left(\frac{5}{11}\right)\neq\left(\frac{5}{13}\right)$, $\left(\frac{17}{11}\right)\neq\left(\frac{17}{13}\right)$ but $\left(\frac{q}{11}\right)=\left(\frac{q}{13}\right)$ for $q=2,3,7$, we observe that either $5|a_i$ or $17|a_i$ for $i\in\mathcal{M}^k$ and either $5\cdot 17|a_i$ or $19|a_i$ or $P(a_i)\leq 7$ for $i\in\mathcal{B}^k$. Since $\sigma_5\leq 3$, we obtain $|\mathcal{M}^k|\leq 4$.

By taking the mirror image (4.4) of (1.1), we may suppose that $0\leq i_{13}\leq 6$ and $0\leq i_{11}\leq 10$. We may assume that $i_{11},a_{13},i_{17},i_{19}$ are not all even otherwise $P(\prod_{i=0}^{5}a_{2i+1})\leq 7$ which is excluded by Lemma 4.1. Further exactly two of $i_{11},a_{13},i_{17},i_{19}$ are even and other two odd otherwise this is excluded again by Lemma 4.1 applied to $\prod^6 i=0(n+i(2d))$ if n is odd and $\prod^6 i=0(\frac{n}{2}+id)$ if $n$is even. Also exactly two of $i_{11},a_{13},i_{17},i_{19}$ lie in each set $\{2,3,4,5,6,7,8\}$, $\{3,4,5,6,7,8,9\}$ and $\{3,4,5,6,7,8,9\}$ otherwise this is excluded by Lemma 4.1.

Since $\max(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\geq 5$ and $|\mathcal{M}^k|\leq 4$, we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|,|\mathcal{I}_2^k|)\leq 4$ and further $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11},i_{13}) for which either $5|a_i$ or $17|a_i$ whenever $i\in\mathcal{M}$. Let $\mathcal{B}'=\mathcal{B}^k\setminus\{i:5\cdot 17|a_i\}$. If $|\mathcal{B}'|\geq 9$, then there are at least 6 elements $i\in\mathcal{B}'$ such that $P(a_i)\leq 3$ giving $k-|R|\geq 2$. Thus we restrict to those pairs for which $|\mathcal{B}'|\leq 8$. For instance, let $(i_{11},i_{13})=(0,0)$. We obtain $\mathcal{M}^k=\{5,10\}$ and $\mathcal{B}^k=\{1,2,3,4,6,7,8,9,12\}$ giving $i_5=0$, $i_{17}\in\{5,10\}$, $\mathcal{B}'=\mathcal{B}^k$ and $|\mathcal{B}^k|=9$. This is excluded.

Let $(i_{11},i_{13})=(1,1)$. Then $\mathcal{M}^k=\{0,6,11\}$ and $\mathcal{B}^k=\{2,3,4,5,7,8,9,10\}$ giving $i_5=1$, $i_{17}=0$. This is excluded. Similarly $(i_{11},i_{13})\in\{(1,3),(2,4),(3,5),(4,6),(6,4),(7,5),(8,6)$ are excluded where we find that i_{17} is of the same parity as i_{11},i_{13}.

Let $(i_{11},i_{13})=(4,2)$. Then $\mathcal{M}^k=\{0,5,10\}$ and $\mathcal{B}^k=\{1,3,6,7,8,9,11,12\}$ giving $5|a_0,5|a_{10}$ and $i_{17}=5$. Further for $i\in\mathcal{B}^k$, we have either $19|a_i$ or $P(a_i)\leq 7$. Also $7|a_1$ and $7|a_8$ otherwise $k-|R|\geq 2$. We now take $(i_7,i_{17})=(1,5)$, $p_1=7,p_2=17$, $\mathcal{I}=\mathcal{B}^k$ and compute $\mathcal{I}_1$ and $\mathcal{I}_2$. Since $\left(\frac{p}{7}\right)=\left(\frac{p}{17}\right)$ for $p\in\{2,3\}$, and $\left(\frac{19}{7}\right)=\left(\frac{19}{17}\right)$, we should have either $|\mathcal{I}_1|=1$ or $|\mathcal{I}_2|=1$. We find that $\mathcal{I}_1=\{3,9,11\}$ $\mathcal{I}_2=\{6,7,12\}$ which is a contradiction. Similarly $(i_{11},i_{13})\in\{(5,3),(8,4)\}$ are also excluded. When $(i_{11},i_{13})=(5,3)$, we find that $i_{17}=6$ and $i_7\in\{0,2\}$ and this is excluded. □

6. A Remark

We consider (1.1) with $\psi=0,\omega(d)=2$ and the assumption $\gcd(n,d)=1$ replaced by $d\nmid n$ if $b>1$. It is proved in [LaSh06a] that (1.1) with $\psi=0,b=1$ and $k\geq 8$ is not possible. We show that (1.1) with $\psi=0,k\geq 6$ and $\omega(d)=2$ is not possible. The case $k=6$ has already been solved in [BBGH06]. Let $k\geq 7$. As in [LaSh06a] and since $d\nmid n$, the assertion follows if (1.1) with $\psi=1$, $k\geq 7$, $\omega(d)=1$ and $\gcd(n,d)=1$ does not hold. This follows from Theorem 1.

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.

[MAGMA] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Jour. Symbolic Comput., **24** (1997), 235-265. Computational algebra and number theory (London, 1993).

[NB02] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, Vol **133** of CWI Tract, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002.

[NB03] N. Bruin. *Chabauty methods using elliptic curves*, J. Reine Angew. Math., **562**, (2003), 27-49.

[LaSh06a] S. Laishram and T. N. Shorey, *The equation* $n(n+d)\cdots(n+(k-1)d) = by^2$ *with* $\omega(d) \leq 6$ *or* $d \leq 10^{10}$, Acta Arith., in press.

[LaSh07] —, *Squares in products in arithmetic progression with at most two terms omitted and common difference a prime power*, to appear

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

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

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

[TSH06] T. N. Shorey, *Powers in arithmetic progression (III)*, The Riemann Zeta function and related themes, Ramanujan Math. Society Publication, (2006), 131-140.

[NSM98] N. P. Smart, emphThe algorithmic resolution of Diophantine equations, volume **41** of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 1998.

[Sz07] Sz. Tengely, *Note on a paper* "An extension of a theorem of Euler" *by Hirata-Kohno et al.*, a preprint.

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, N2L3G1, Canada

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

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India

E-mail address: shorey@math.tifr.res.in

Mathematical Institute, University of Debrecen, Hungary

E-mail address: tengely@math.klte.hu