ACTA ARITHMETICA
135.2 (2008)

Squares in products in arithmetic progression with at most one term omitted and common difference a prime power

by

Shanta Laishram (Waterloo, ON),
T. N. Shorey (Mumbai) and Szabolcs Tengely (Debrecen)

1. Introduction. For an integer $x > 1$, we denote by $P(x)$ and $\omega(x)$ the greatest prime factor of x and the number of distinct prime divisors of x, respectively. Further, we put $P(1) = 1$ and $\omega(1) = 0$. Let p_i be the ith prime number. Let $k \geq 4$, $t \geq k-2$ and $\gamma_1 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Thus $t \in \{k, k-1, k-2\}$, $\gamma_t \geq k-3$ and $\gamma_i = i-1$ for $1 \leq i \leq t$ if $t = k$. We put $\psi = k - t$. Let b be a positive squarefree integer and we shall 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 [SaSh03] and [MuSh04]) 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 [SaSh03] and [MuSh04]) 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.

2000 *Mathematics Subject Classification*: Primary 11D61.

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

Research of Sz. Tengely was supported in part by the Magyary Zoltán Higher Educational Public Foundation.

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 [LaSh08].

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

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

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

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

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

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

Let

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

Lemma 2.1 ([LaSh08]). *Equation* (1.1) *with* $\omega(d) = 1$ *and* $k \geq 9$ *implies that* $t - |R| \leq 1$.

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

This is proved in [SaSh03] and [MuSh03] unless $k = 5$, $P(b) = 5$, and then it is a particular case of a result of Tengely [Sz08].

Lemma 2.3 ([SaSh03, Theorem 4] and [MuSh04]). *Let* $\psi = 1$, $k \geq 9$ *and* $d \nmid n$. *Assume that* $P(b) < k$. *Then* (1.1) *with* $\omega(d) = 1$ *does not hold.*

Lemma 2.4 ([LaSh08]). *Let* $\psi = 2$, $k \geq 15$ *and* $d \nmid n$. *Then* (1.1) *with* $\omega(d) = 1$ *does not hold.*

Lemma 2.5. *Let* $\psi = 1$, $k = 7$ *and* $d \nmid n$. *Assume that* (1.1) *holds. Then* $(a_0, a_1, \dots, a_6)$ *is different from the following tuples and their mirror images*:

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

Further, $(a_1, \dots, a_6)$ *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*

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

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* $a_2 = 2$, $a_4 = 6$, $a_5 = 5$ *hold*,
(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* $a_1 = 5$, $a_2 = 6$, $a_4 = 2$ *hold*,
(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* $a_1 = 2$, $a_3 = 6$, $a_6 = 3$ *hold.*

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 an integral point on it. Then we compute all integral points on the curve by using the MAGMA command *IntegralQuarticPoints* and we exclude them.

We illustrate this with an example. 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

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

or

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

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

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

When $a_2 = 2$, $a_4 = 6$, by putting $X = x_1 + 1$, $Y = 6x_2x_4$, 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 find by using the 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 $Y=10x_2x_5$, we get the curve $Y^2=10(X^2+4)((X+3)^2+4)=10X^4+60X^3+170X^2+240X+520$ on which $(X,Y)=(-1,20)$ is an integral point. It follows by MAGMA that all the integral points on the curve satisfy $X\leq 1$, and also this case is excluded. When $a_4=6$, $a_5=5$, by putting $X=x_1+3$ and $Y=30x_4x_5$, we get the curve $Y^2=30(X^2+6)((X+1)^2+4)=30X^4+60X^3+330X^2+360X+900$ on which $(X,Y)=(0,30)$ is an integral point. It follows by MAGMA that all the integral points on the curve other than $(X,Y)=(11,500)$ satisfy $X\leq 1$. Since $X>1$, $30\,|\,Y$ and $30\nmid 500$, also this case is excluded. When (2.5) holds, we get $5d=2x_1+1$, and this with $n+d=x_1^2$ implies

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

As in the case (2.4), these give 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 case (iii), we have $n=2x_0^2$ and obtain either $d=2x_0+3$ or $3d=2x_0+1$. Then we use $2a_ix_i^2=2(n+id)=(2x_0)^2+2i(2x_0+3)=(2x_0+i)^2+6i-i^2$ 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 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 $\mathrm{ord}_3(X^4+6X^3+18X-9)=2$, giving $\mathrm{ord}_3(Y^2)=\mathrm{ord}_3(6)+2=3$, a contradiction. ∎

3. Proof of Lemma 2.5. For the proof of Lemma 2.5, we use the so-called elliptic Chabauty method (see [NB02], [NB03]). Bruin's routines related to the elliptic Chabauty method are contained in [MAGMA], so here we indicate the main steps only, and a MAGMA routine which can be used to verify the computations is available from the third author.

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

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

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

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

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 find 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 deduce 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 $p = 23$ shows 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 only point on $C_{-10+5\sqrt{3}}$ for which $X \in \mathbb{Q}$ is $(X, Y) = (-1/3, 0)$.

We have proved that there is no arithmetic progression with $(a_0, a_1, \ldots, a_6) = (6, 7, 2, 1, 10, *, 3)$ and $d \nmid n$.

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

$$x_6^2 - 3x_1^2 = -2(x_0/2)^2, \quad 4x_6^2 + 3x_1^2 = 7x_3^2,$$
$$x_6^2 + 2x_1^2 = 3x_2^2, \quad 3x_6^2 + x_1^2 = x_4^2.$$

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

$$x_6 + \sqrt{3}\,x_1 = \delta_1\square, \qquad \frac{\sqrt{-3}\,x_6 + x_1}{2} = \delta_2\square,$$

where

$$\delta_1 \in \{\pm 1 + \sqrt{3}, \pm 1 - \sqrt{3}, \pm 5 + 3\sqrt{3}, \pm 5 - 3\sqrt{3}\},$$
$$\delta_2 \in \{\pm 1, (\pm 1 + \sqrt{-3})/2, (\pm 1 - \sqrt{-3})/2\}.$$

The curves for which we apply the elliptic Chabauty method are

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

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

We now make some observations. If

$$u(n+id) + v(n+jd) = w(n+ld) \tag{3.2}$$

holds with $0 \le i, j, l \le k-1$ and integers u, v, w, then

$$u + v = w \quad \text{and} \quad ui + vj = wl.$$

Therefore

$$u(n+(k-1-i)d) + v(n+(k-1-j)d) = w(n+(k-1-l)d)$$

holds, and vice versa. Therefore any tuple $(a_0, a_1, \dots, a_6)$ and its mirror tuple $(a_6, \dots, a_1, a_0)$ give rise to the same set of equations. Hence it suffices to exclude any one of them. Also it suffices to exclude any one of $(*, a_1, \dots, a_6)$ and $(a_0, a_1, \dots, a_5, *)$.

Further, if we define $a'_i = a_i/2$ if a_i is even and $a'_i = 2a_i$ if a_i is odd, then $(a'_0, a'_1, \dots, a'_6)$ and $(a_0, a_1, \dots, a_6)$ give rise to the same set of equations. Let i, j, l satisfy (3.2). If $n+id = a_i x_i^2$, $n+jd = a_j x_j^2, n+ld = a_l x_l^2$ is the one given by $(a_0, a_1, \dots, a_6)$, and $n+id = a'_i x_i'^2$, $n+jd = a'_j x_j'^2$, $n+ld = a'_l x_l'^2$ the one given by $(a'_0, a'_1, \dots, a'_6)$, then from (3.2) we get

$$u a_i x_i^2 + v a_j x_j^2 = w a_l x_l^2 \tag{3.3}$$

and

$$u a'_i x_i'^2 + v a'_j x_j'^2 = w a'_l x_l'^2, \tag{3.4}$$

respectively. Since $2a'_i x_i'^2 = a_i y_i^2$ for some y_i, multiplying (3.4) by 2, we obtain an equation exactly similar to (3.3). Hence if we exclude one of $(a'_0, a'_1, \dots, a'_6)$ or $(a_0, a_1, \dots, a_6)$, the other tuple is excluded.

In view of the above observations and since $(a_0, a_1, \dots, a_6) = (1, 2, 3, *, 5, 6, 7)$ is excluded if $(a_1, a_2, \dots, a_6) = (1, 2, 3, *, 5, 6)$ is excluded, it suffices to consider the tuples

$$(a_0, a_1, \dots, a_6) \in \{(*, 3, 1, 5, 6, 7, 2), (3, *, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, *, 10), (*, 5, 6, 7, 2, 1, 10), (6, 7, 2, 1, 10, *, 3), (*, 1, 2, 3, *, 5, 6)\}.$$

Already the tuples $(a_0, a_1, \dots, a_6) \in \{(1, 5, 6, 7, 2, *, 10), (6, 7, 2, 1, 10, *, 3)\}$ are excluded. In the table below, we indicate the relevant quartic polynomials for the remaining tuples:

Tuple	Polynomial
$(1, 2, 3, *, 5, 6)$	$2\delta_{A1}(X+\sqrt{-1})(X+3\sqrt{-1})(5X^2-3)$
$(*, 3, 1, 5, 6, 7, 2)$	$\delta_{A2}(X+\sqrt{-1})(2X+\sqrt{-1})(5X^2-1)$
$(3, *, 5, 6, 7, 2, 1)$	$5\delta_{A3}(2X+3\sqrt{-1})(X+\sqrt{-1})(12X^2-3)$
$(*, 5, 6, 7, 2, 1, 10)$	$\delta_{A4}(X+\sqrt{-2})(2\sqrt{-2}\,X+1)(3X^2+1)$

∎

4. Proof of Theorem 1. Suppose that the assumptions of Theorem 1 are satisfied and assume (1.1) with $\omega(d) = 1$. Let $k \ge 9$. By Lemma 2.3, we may suppose that $P(b) = k$, implying k is a prime. After deleting the term divisible by k on the left hand side of (1.1) and using Lemma 2.4, the assertion for $k \ge 15$ follows. Thus it suffices to prove the assertion for $k \in \{7, 8, 11, 13\}$ with $P(b) \le k$ for $k \in \{7, 8\}$ and $P(b) = k$ for $k \in \{11, 13\}$. Therefore we always restrict to $k \in \{7, 8, 11, 13\}$ and $P(b) \le k$ for $k \in \{7, 8\}$ and $P(b) = k$ for $k \in \{11, 13\}$. In view of Lemma 2.1, we arrive at a contradiction by showing $t - |R| \ge 2$ when $k \in \{11, 13\}$. Further, Lemma 2.1 also implies that $p \nmid d$ for $p \le k$ 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 $p \mid n + i_p d$. 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

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

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

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

or

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

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

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

and

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

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

$$(m - \gamma'_1 d) \cdots (m - \gamma'_t d) = by^2. \tag{4.4}$$

The equation (4.4) is called the mirror image of (1.1). The corresponding t-tuple $(a_{\gamma'_1}, \ldots, a_{\gamma'_t})$ is called the mirror image of $(a_{\gamma_1}, \ldots, a_{\gamma_t})$.

4.1. *The case* $k = 7,\ 8$. 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 $n + id > 24i$, since $n > 208$ if $d \le 23$. 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 $a_i x_i^2 = n + id > 24i \ge 4i^2$, we get

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

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 $8 \mid d$. From (2.1), we get $\left(\frac{a_i}{8}\right) = \left(\frac{n+id}{8}\right) = \left(\frac{n}{8}\right)$, implying a_i's belong each to exactly one distinct residue class modulo 8. Therefore $|\{a_i : P(a_i) \le 5\}| \le 1$, which together with $|\{j : a_j = a_i\}| \le 2$ for $a_i \in R$ implies $|\{i : P(a_i) \le 5\}| \le 2$. 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 [LaSh07, Corollary 3.10] that $d_2 = d < 24$ and $n + 5d < 324$. This is not possible.

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

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

Let $p_1 = 5$, $p_2 = 7$ and $\mathcal{I} = \{\gamma_1, \ldots, \gamma_6\}$. We observe that $P(a_i) \le 3$ for $i \in \mathcal{M} \cup \mathcal{B}$. Since $\left(\frac{2}{5}\right) \ne \left(\frac{2}{7}\right)$ 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

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

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

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

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

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 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 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 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 $0 \le i_5 < 5$ and $0 \le i_7 \le 3$, 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 $\max(|\mathcal{I}^k_1|, |\mathcal{I}^k_2|)$ ≤ 4. Then we check for the possibilities I, II, III or IV.

Suppose $d = 2p^\alpha$. Then $b_i \in \{1, 3\}$ whenever $P(b_i) \le 3$. If $i_5 \ne 0, 1$, then $|R| \le 2 + 2 = 4$, giving $t - |R| \ge 7 - 1 - 4 = 2$, 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 $|\mathcal{I}^k_1| \le 1$ or $|\mathcal{I}^k_1| \le 2$. 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 cases III and IV, since $b_i \in \{1, 3\}$ whenever $P(b_i) \le 3$. Suppose III holds. Then by reducing modulo 3, we obtain $4 \notin \mathcal{I}$, $a_6 = 3$ and $a_2 = a_3 = 1$. By reducing 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 reducing 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 as $t - |R| \le 1$, we get $a_1 = 7$. This is not possible since $-1 = \left(\frac{a_1 a_4}{5}\right) = \left(\frac{(1-0)(4-0)}{5}\right) = 1$. 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 $1 \in \mathcal{I}$, as otherwise $P(a_2 a_3 a_4 a_5 a_6) \le 5$ and this is excluded by Lemma 2.2 with $k = 5$. Further, $i \notin \mathcal{I}$ for exactly one of $i \in \{2, 3, 4\}$, as otherwise $P(a_1 a_2 a_3 a_4) \le 3$ and this is not possible by Lemma 2.2 with $k = 4$ since $d > 23$. Consider the possibilities II and IV. By reducing modulo 3, we obtain $2 \notin \mathcal{I}$, $3 \mid a_1 a_4$ and $a_3 a_6 = 2$. This is not possible modulo 3 since $-1 = \left(\frac{a_3 a_6}{3}\right) = \left(\frac{(3-1)(6-1)}{3}\right) = 1$, 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, which 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 reducing modulo 2 and 3. Thus we have $(a_1, \ldots, a_5, a_6) = (1, 2, 3, *, 5, 6)$.

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 reducing modulo 2 and 3. Thus $(a_1, \ldots, a_5, a_6) = (2, 1, 6, *, 10, 3)$ 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 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 reducing 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 reducing modulo 3. By reducting modulo 3, we get $a_5 \in \{2, 5\}$ and we may take $a_5 = 5$, as 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 reducing 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 reducing modulo 3. This is not possible modulo 7 since $-1 = \left(\frac{a_4 a_5}{7}\right) = \left(\frac{(4-3)(5-3)}{7}\right) = 1$. Thus $a_1 = 2$, $6 \notin \mathcal{I}$. Then $a_0 = 5$, $a_5 = 10$, $a_3 = 14$ by reducing modulo 3, giving $(a_0, a_1, \ldots, a_5, a_6) = (5, 2, 1, 14, 3, 10, *)$. 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 $7 \,|\, a_3$, as otherwise $P(a_1 a_2 \ldots a_5) \leq 5$ if $1 \in \mathcal{I}$ or $P(a_2 a_3 \ldots a_6) \leq 5$ if $6 \in \mathcal{I}$, and this is excluded by Lemma 2.2 with $k = 5$. Further, by reducing 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 a parity argument, we have either $5 \notin \mathcal{I}$ or $4 \notin \mathcal{I}$. Again by reducing 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 $5 \,|\, a_1$, as otherwise we get a contradiction from $P(a_1 a_2 a_3 a_4) \leq 3$, Lemma 2.2 with $k = 4$ and $d > 23$. Hence $a_1 = 5$. This is again a contradiction since $-1 = \left(\frac{a_1 a_2}{7}\right) = \left(\frac{(1-0)(2-0)}{7}\right) = 1$. Thus the possibility I is excluded. If 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 reducing 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 by further reducing 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 reducing 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 reducing modulo 2 and 3 and we get $P(a_2a_3 \ldots a_6) \le 5$, which is excluded by Lemma 2.2 with $k = 5$. Let II hold. Then $3 \notin \mathcal{I}$ by reducing 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 reduction 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 $i \in \{0, 2, 4, 6\}$, as otherwise n is even, $P(a_0a_2a_4a_6) \le 3$ and this is excluded by $k = 4$ of Lemma 2.2 applied to $(n/2)(n/2 + d)(n/2 + 2d)(n/2 + 3d)$. We consider the possibilities I and III. By reducing modulo 3, we get $4 \notin \mathcal{I}$, $a_0 = a_6$, $3 \mid a_0$ and $a_2a_5 = 2$. This is not possible by reducing modulo 3. Next we consider the possibility II. Then $4 \notin \mathcal{I}$ by a parity argument. Further, $a_0 = a_6 = 1$, $a_2 = 3, a_5 = 6$. This is not possible since $8 \mid x_6^2 - x_0^2 = n + 6d - n = 6d$ 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 $a_2 = 6$ and $a_4 = 1$. 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 reduction 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 $\mathcal{A}_7 = (1, 2, 3, *, 5, 6, 7)$ or $(5, 6, 7, 2, 1, 10, *)$ or $(10, 3, 14, 1, 2, 5, *)$, which are all 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 $a_1 = 5$, $a_2 = 6$, $a_4 = 2$ hold, 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 impossible by 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 $a_1 = 2, a_3 = 6, a_6 = 3$ hold. 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 $11 \mid a_i$ for some $i \in \{4, 5, 6\}$ whenever $i \notin \mathcal{I}$, as otherwise the lemma follows from Lemma 4.1.

Let $p_1 = 5$, $p_2 = 11$ and $\mathcal{I} = \{\gamma_1, \ldots, \gamma_t\}$. 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 $3 \mid a_i$ whenever $i \in \mathcal{M}$. Since $\sigma_3 \le 4$ and $|\mathcal{I}| = k - 1$, we deduce from (4.3) that $|\mathcal{M}^k| \le 5$ and $3 \mid a_i$ for at least $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$. Further, $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{B}$, giving $|\mathcal{B}| \le 5$, as 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 $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$ and restrict to those pairs (i_5, i_{11}) for which $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \le 6$. Further, we restrict to those pairs (i_5, i_{11}) for which either

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

or

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

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 $3 \mid a_i$ 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 three elements $i \in \mathcal{B}^k$ with $P(a_i) \le 2$, as otherwise $t - |R| \ge 2$. 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 $|\mathcal{B}^k| \ge 5$. Hence we may suppose that $7 \mid a_i$ for some $i \in \mathcal{B}$, as otherwise $a_i \in \{1, 2\}$ for $i \in \mathcal{B}$, which together with $|\mathcal{B}| \ge 4$ gives $t - |R| \ge 2$. Further, if $|\mathcal{B}^k| = 6$, then we may assume that $7 \mid a_i, 7 \mid a_{i+7}$ for some $0 \le i \le 3$.

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 $7 \mid a_6 a_7$, then $|\mathcal{B}| = |\mathcal{B}^k| - 1$ and $a_i \in \{3, 6\}$ for $i \in \mathcal{M} = \mathcal{M}^k$ but $\left(\frac{a_3 a_9}{7}\right) = \left(\frac{(3 - i_7)(9 - i_7)}{7}\right) = -1$ for $i_7 = 6, 7$, a contradiction. If $7 \mid a_2$, then $a_i \in \{5, 10\}$ for $i \in \{5, 10\} \subseteq \mathcal{I}$ but $\left(\frac{a_5 a_{10}}{7}\right) = \left(\frac{(5-2)(10-2)}{7}\right) = -1$, a contradiction again. Thus $7 \mid a_1 a_8$ 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 $7 \mid a_0 a_7$ or $7 \mid a_2 a_9$. Taking $\left(\frac{a_i}{7}\right)$ for $i \in \{4, 10, 0, 2, 3, 7, 8, 9\}$, we find that $7 \mid a_2 a_9$ 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, $7 \mid a_1a_8$ or $7 \mid a_3a_{10}$. Taking $\left(\frac{a_i}{7}\right)$ for $i \in \mathcal{M} \cup \mathcal{B}^k$, we find that $7 \mid a_1a_8$ 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 $13 \mid a_3a_4a_5a_6a_7a_8a_9$, otherwise the assertion follows from Theorem 1 with $k = 11$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \ldots, \gamma_t\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q = 2, 3, 7$, we observe that for $5 \mid a_i$ 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 $5 \mid a_i$ for at least $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$.

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 $i_{11} \geq 2$, as 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 $5 \mid a_i$ for at least $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$. If $5 \mid a_i$ for exactly $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$, then $\mathcal{B} = \mathcal{B}^k$ and hence we may assume that $|\mathcal{B}| = |\mathcal{B}^k| \leq 7$, as otherwise there are at least six 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 $5 \mid a_i$ 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 $p_{\pi(k)+1} \mid b$. 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 $p \mid a_i$ with $p \in \{13, 17\}$ when $k = 11$ and $p \mid a_i$ with $p \in \{17, 19\}$ when $k = 13$, we observe 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 $\mathcal{I} = \{0, 1, \ldots, 10\}$. 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 $5 \mid a_i$ or $17 \mid a_i$ for $i \in \mathcal{M}$ and either $5 \cdot 17 \mid a_i$ 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, as otherwise we get a contradiction from Lemma 4.1 applied to $\prod_{i=0}^{5} (n + i(2d))$. Also we may suppose that $\max(i_{11}, i_{13}) \geq 4$, as otherwise we get a contradiction from Lemma 4.1 applied to $\prod_{i=0}^{6} (n + 4d + id)$. 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 $5 \mid a_i$ or $17 \mid a_i$ whenever $i \in \mathcal{M}$. Let $\mathcal{B}' = \mathcal{B} \setminus \{i : 5 \cdot 17 \mid a_i\}$. If $|\mathcal{B}'| \geq 8$, then there are at least six 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 $7 \mid a_i$ and $7 \mid a_{i+7}$ 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 $i_5 = 1$, $17 \mid a_8$ 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 $5 \mid a_2 a_7$, $17 \mid a_9$ 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 $5 \mid a_5, 17 \mid a_9$ or $17 \mid a_5, 5 \mid a_9$. 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 $i_5 = 2$, $17 \mid a_0$ 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 reducing modulo 7, we get $a_i \in \{1, 2\}$ for $i \in \{1, 8, 9\}$ and $a_5 \in \{3, 6\}$. Further, by reducing modulo 5, we obtain $a_1 = a_8 = 1$, $a_9 = 2$, $a_5 = 3$, $a_1 = 4$, $a_{10} = 7$, and this is excluded by Runge's method as in [MuSh03]. 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 $5 \mid a_0 a_5 a_{10}$ 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 $\mathcal{I} = \{0, 1, \dots, 12\}$. 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 $5 \mid a_i$ or $17 \mid a_i$ for $i \in \mathcal{M}^k$ and either $5 \cdot 17 \mid a_i$ or $19 \mid a_i$ 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 $i_{11}, i_{13}, i_{17}, i_{19}$ are not all even, as otherwise $P(\prod_{i=0}^{5} a_{2i+1}) \leq 7$, which is excluded by Lemma 4.1. Further, exactly two of $i_{11}, i_{13}, i_{17}, i_{19}$ are even and the other two odd, as otherwise this is excluded again by Lemma 4.1 applied to $\prod_{i=0}^{6}(n + i(2d))$ if n is odd and $\prod_{i=0}^{6}(n/2 + id)$ if n is even. Also exactly two of $i_{11}, i_{13}, i_{17}, i_{19}$ lie in each set $\{2, 3, 4, 5, 6, 7, 8\}$ 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 $5 \mid a_i$ or $17 \mid a_i$ whenever $i \in \mathcal{M}$. Let $\mathcal{B}' = \mathcal{B}^k \setminus \{i : 5 \cdot 17 \mid a_i\}$. If $|\mathcal{B}'| \geq 9$, then there are at least six 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 $5 \mid a_0$, $5 \mid a_{10}$ and $i_{17} = 5$. Further, for $i \in \mathcal{B}^k$, we have either $19 \mid a_i$ or $P(a_i) \leq 7$. Also $7 \mid a_1$ and $7 \mid a_8$, as 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 [LaSh07] 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 [LaSh07] 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*, J. Symbolic Comput. 24 (1997), 235–265.

[NB02] N. Bruin, *Chabauty Methods and Covering Techniques Applied to Generalized Fermat Equations*, CWI Tract 133, Stichting Math. Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002.

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

[LaSh07] 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. 129 (2007), 249–305.

[LaSh08] —, —, *Squares in arithmetic progression with at most two terms omitted*, ibid. 134 (2008), 299–316.

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

[MuSh04] —, —, *Almost squares in arithmetic progression (III)*, Indag. Math. 15 (2004), 523–533.

[SaSh03] N. Saradha and T. N. Shorey, *Almost squares in arithmetic progression*, Compos. Math. 138 (2003), 73–111.

[TSH06] T. N. Shorey, *Powers in arithmetic progression (III)*, in: The Riemann Zeta Function and Related Themes, Ramanujan Math. Soc. Publ., 2006, 131–140.

[Sz08] Sz. Tengely, *Note on a paper "An extension of a theorem of Euler" by Hirata-Kohno et al. (Acta Arith. 129 (2007), 71–102)*, Acta Arith. 134 (2008), 329–335.

Department of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo, ON, N2L 3G1, Canada
E-mail: shanta@math.tifr.res.in

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

Institute of Mathematics
University of Debrecen
and the Number Theory Research Group
of the Hungarian Academy of Sciences
P.O. Box 12, 4010 Debrecen, Hungary
E-mail: tengely@math.klte.hu

Received on 19.12.2007
and in revised form on 4.8.2008 (5598)