Compositio Mathematica **138:** 73–111, 2003.



# Almost Squares in Arithmetic Progression

N. SARADHA and T. N. SHOREY
*School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India. e-mail: {saradha, shorey}@math.tifr.res.in*

(Received: 29 May 2001; accepted in final form: 22 March 2002)

**Abstract.** It is proved that a product of four or more terms of positive integers in arithmetic progression with common difference a prime power is never a square. More general results are given which completely solve (1.1) with $\gcd(n, d) = 1, k \geqslant 3$ and $1 < d \leqslant 104$.

**Mathematics Subject Classification (2000).** Primary: 11D61.

**Key words.** arithmetic progressions, congruences, diophantine equations, elliptic equations, Legendre symbol, squarefree integers.

## 1. Introduction

We shall always denote by $n, d, k, b, y$ positive integers such that $b$ is square free, $k \geqslant 2$ and $P(b) \leqslant k$, where $P(b)$ denotes the greatest prime factor of $b$ with the understanding that $P(1) = 1$. We consider the equation

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

For a survey of results on (1.1), we refer to [14, 15, 18]. We observe that (1.1) with $k = 2$ has infinitely many solutions. The first result on (1.1) is due to Fermat (see [6, pp. 21–22] or [1, p. 440]) that there are no four squares in an arithmetic progression. Further, Euler (see [1, p. 635]) proved that (1.1) with $\gcd(n, d) = 1, k = 4, b = 1$ is not possible. This is also the case if $k = 5, b = 1$ by a result of Obláth [7].

Let $d = 1$ and $k \geqslant 3$. It is a consequence of some old diophantine results that (1.1) with $k = 3$ is possible only when $n = 1, 2, 48$. If $P(b) < k$ and $k \geqslant 4$, Erdős and Selfridge [3], developing on the work of Erdős [2] and Rigge [8], showed that (1.1) with $n > k^2$ does not hold. The assumption $P(b) < k$ has been relaxed to $P(b) \leqslant k$ and $P(b) \leqslant p_k$ in [10] and [13], respectively, where $p_k$ denotes the least prime exceeding $k$. Furthermore, it is shown in [13] that for $n > k^2, k \geqslant 4$ and $(n, k) \neq (24, 4), (47, 4), (48, 4)$ there exist distinct primes $p_1$ and $p_2$ such that the maximal power of each of $p_1$ and $p_2$ dividing the left-hand side of (1.1) is odd. This finds application in the proof of Theorem 1 stated below. We observe that the assumption $n > k^2$ in the above results is necessary otherwise we see from (1.1) that $P(y) \leqslant k$ and (1.1) has infinitely many solutions. Finally, we see that $n > k^2$ follows if (1.1) holds such that the left-hand side is divisible by a prime exceeding $k$.

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Let $d > 1$ and $k \geqslant 3$. Then the assumption $n > k^2$ is no longer necessary since the left-hand side of (1.1) with $\gcd(n, d) = 1$ is divisible by a prime exceeding $k$ unless $(n, d, k) = (2, 7, 3)$. This was proved by Shorey and Tijdeman [17]. Marszalek [5] showed that (1.1) with $\gcd(n, d) = 1, b = 1$ implies that $k$ is bounded by an effectively computable number depending only on $d$. Further, Shorey and Tijdeman [16] showed that (1.1) with $\gcd(n, d) = 1$ is not possible if $k$ exceeds an effectively computable number depending only on $\omega(d)$ where $\omega(1) = 0$ and $\omega(d)$ denotes the number of distinct prime divisors of $d$.

Let

$$\mathcal{D} = \{\chi\tau^{\alpha} \mid \chi, \alpha \text{ integers with } 1 \leqslant \chi \leqslant 12, \chi \neq 11, \alpha > 0, \tau \text{ prime}, \gcd(\chi, \tau) = 1\}. \tag{1.2}$$

We shall always write $\tau = p$ if $\tau > 2$. We observe that every $d$ with $1 < d \leqslant 104$ is an element of $\mathcal{D}$ and $\omega(d) \leqslant 2$ for $d \in \mathcal{D}$ unless $\chi = 6, 10, 12$ in which case $\omega(d) = 3$. We restrict (1.1) to $d \in \mathcal{D}$ in this paper. We observe that (1.1) with $\gcd(n, d) = 1, d \in \mathcal{D}$ and $k = 2$ has infinitely many solutions if $d$ is odd or $8 \mid d$ otherwise there is no solution. Thus we assume that $k \geqslant 3$ from now on. The first result is on (1.1) with $d = p^{\alpha}$ and $P(b) < k$.

THEOREM 1. *Let* $d = p^{\alpha}$. *Assume* (1.1) *with* $P(b) < k$. *We have*

(i) *If* $b = 1$, *then* $k = 3$.
(ii) *If* $d \nmid n$, *then* $k \leqslant 9$.

Assume (1.1) with $\gcd(n, d) = 1, b = 1, d = p$ and $k = 3$. Then we observe that either

$$n = y_0^2, \quad n + d = y_1^2, \quad n + 2d = y_2^2 \quad \text{or} \quad n = 2y_0^2, \quad n + d = y_1^2,$$
$$n + 2d = 2y_2^2$$

for some positive integers $y_0, y_1, y_2$ which are pairwise coprime. Assume the first possibility. Then $y_1^2 - y_0^2 = d$ and $y_2^2 - y_1^2 = d$. This implies that $y_1 - y_0 = 1, y_1 + y_0 = d$ and $y_2 - y_1 = 1, y_2 + y_1 = d$ since $d = p$. Thus $y_0 = y_2$ which is not possible. Now we turn to the second possibility. Then $y_2^2 - y_0^2 = d$ implying that $y_2 - y_0 = 1$ and $y_2 + y_0 = d$. Thus $y_0 = (d-1)/2$ which gives $n = (d-1)^2/2$ and since $n + d = y_1^2$, we get $d^2 - 2y_1^2 = -1$. We do not know whether the preceding equation has infinitely many solutions in $d, y_1$ with $d$ prime. Thus it is an open problem that (1.1) with $b = 1, d = p$ and $k = 3$ has infinitely many solutions.

Let $k$ be even. We write $k! = bz^2$ where $b$ is square free and we observe that $P(b) < k$. Now we see that the left hand side of (1.1) with $n = d$ is $by^2$ where $y = zd^{\frac{k}{2}}$. Thus the assumption $d \nmid n$ is necessary in Theorem 1(ii). This is also the case when $k$ is odd by considering (1.1) with $n = d = k$.

Next we give a result on (1.1) with $d \neq p^{\alpha}$ and $P(b) < k$.

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

THEOREM 2. *Let* $d \in \mathcal{D}$, $d \neq p^\alpha$ *and* $P(b) < k$. *Assume* (1.1) *such that* $d \nmid n$ *if* $d = 2^\alpha$ *and* $\chi \nmid n$ *otherwise. Then* $k = 3$ *or* $k = 5, \chi = 10, 5 \mid n, 2 \nmid n$ *or* $(n, d, k) = (4 \cdot 11^\alpha, 7 \cdot 11^\alpha, 5)$ *with* $\alpha$ *odd.*

We consider an analogue of Theorem 2 with $\chi \mid n$. Then we should assume that $d \nmid n$ as mentioned above. Thus we suppose that $\tau^\alpha \nmid n$. Now we divide both sides of (1.1) by $\chi^k$ to suppose that $d = \tau^\alpha$ and we conclude by Theorem 2 for $\tau = 2$ and by Theorem 1(ii) for $\tau > 2$ that $k \leqslant 9$. If the assumption $\chi \nmid n$ is replaced by $\gcd(n, d) = 1$ in Theorem 2, then either $k = 3, d = 7p^\alpha$ or $(n, d, k) = (1, 24, 3)$, see Corollary 4(iii). Like (1.1) with $k = 3$ and $d = p$, the case $k = 3, d = 7p$ also remains open. If $k = 3$ in Theorem 2, we observe that (1.1) has infinitely many solutions $(n, d) = (2^{\alpha-3}, 3 \cdot 2^\alpha), (2^{\alpha+1}, 7 \cdot 2^\alpha), (9 \cdot 2^{\alpha+1}, 7 \cdot 2^\alpha)$. This is also the case with the second possibility in the assertion of Theorem 2. For this, we observe $(n, d, k) = (5 \cdot 7^\alpha, 10 \cdot 7^\alpha, 5)$ with $\alpha$ odd are solutions of (1.1). The second possibility is ruled out if $\gcd(n, \chi) = 1$ and the third possibility is excluded if $\gcd(n, d) = 1$. Now we give a result on (1.1) with $P(b) = k$.

THEOREM 3. *Let* $d \in \mathcal{D}$ *and* $k$ *be prime. Then* (1.1) *with* $\gcd(n, d) = 1$ *and* $P(b) = k$ *implies that* $k \leqslant 29, d = p^\alpha$ *or* $k = 3, d = 7p^\alpha$.

The main purpose of this paper is to consider (1.1) when $d$ runs through an explicitly given infinite set including all prime powers and Theorems 1, 2, 3 are results in this direction. Further we find large $d_0$ such that (1.1) with $\gcd(n, d) = 1$ can be solved completely for $1 < d \leqslant d_0$. For elaborating this application, we show in the next result that $d_0$ can be taken as 104. This is not the optimal value of $d_0$ obtainable by the method of this paper.

COROLLARY 1. *All the solutions of* (1.1) *with* $\gcd(n, d) = 1$ *and* $1 < d \leqslant 104$ *are given by* $(n, d) \in \{(2, 7), (18, 7), (64, 17), (2, 23), (4, 23), (75, 23), (98, 23), (338, 23), (3675, 23), (1, 24), (800, 41), (2, 47), (27, 71), (50, 71), (96, 73), (864, 97)\}$ *if* $k = 3$; $(n, d) \in \{(75, 23)\}$ *if* $k = 4$.

Saradha [11] proved Corollary 1 when $d \leqslant 22$ and Filakovszky and Hajdu [4] covered $23 \leqslant d \leqslant 30$.

We derive Theorem 3 from the following result.

THEOREM 4. *Let* $d \in \mathcal{D}$, $\gcd(n, d) = 1$, $P(b) < k, k \geqslant 4$ *and* $i$ *be any integer with* $0 < i < k - 1$. *Then*

$$n(n + d) \cdots (n + (i - 1)d)(n + (i + 1)d) \cdots (n + (k - 1)d) = by^2 \tag{1.3}$$

*implies that either* $(n, d, k, i) \in \{(1, 8, 4, 2), (1, 40, 4, 1), (25, 48, 4, 1)\}$ *or* $d \in \{p^\alpha, 5p^\alpha, 7p^\alpha\}$ *such that* $k \leqslant 29$ *if* $d = p^\alpha$ *and* $k \leqslant 5$ *if* $d = 5p^\alpha, 7p^\alpha$.

We observe that (1.3) with $b = 1, k = 3$ has infinitely many solutions unless $2 \parallel d$ in which case it has no solution. The case $d = 1$ of Theorem 4 is given in [13] where we proved that (1.3) with $d = 1, n > k^2, P(b) \leqslant k, k \geqslant 4$ and $0 < i < k - 1$ implies that

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

$(n, k, i) = (24, 4, 2)$. This result has been applied in [13] to settle a question of Erdős and Selfridge [3, p. 300] that there is no square other than $12^2 = \frac{6!}{5}$ and $720^2 = \frac{10!}{7}$ such that it can be written as a product of $k - 1$ integers out of $k$ consecutive positive integers. For $1 < d \leqslant 67$, we solve (1.3) completely in the next result.

COROLLARY 2. *Let* $1 < d \leqslant 67$ *and* $i$ *be an integer with* $0 < i < k - 1$. *Then* (1.3) *with* $\gcd(n, d) = 1$, $P(b) < k$ *and* $k \geqslant 4$ *implies that*

$$k=4 \quad \text{and} \quad (n,d) \in \{(1,5),(3,5),(49,5),(4,7),(1,8),(3,11),(36,13),(108,13),$$
$$(27,23),(75,23),(288,25),(363,29),(2116,31),(289,37),(1,40),(400,43),$$
$$(3,47),(6,47),(75,47),(484,47),(1587,47),(25,48),(7744,59),(900,61)\};$$
$$k=5 \quad \text{and} \quad (n,d) \in \{(4,7),(4,23)\};$$
$$k=6 \quad \text{and} \quad (n,d) \in \{(5,11)\}.$$

Corollaries 1 and 2 with $d = \chi$ have been used in relaxing the assumption $\gcd(n, d) = 1$ in Corollary 4(iii) to $\chi \nmid n$ in Theorem 2. Another application of Corollaries 1 and 2 is given as follows. Let $1 < d \leqslant 67$, $k \geqslant 4$ and $\gcd(n, d) = 1$. Suppose that there exists exactly one prime $p \geqslant k$ dividing the left-hand side of (1.1) to an odd power. This means we have

$$n(n + d) \cdots (n + (k - 1)d) = bpy^2 \tag{1.4}$$

for some positive integers $b$ and $y$ such that $b$ is square free and $P(b) < k$. We delete the one term divisible by $p$. If $p \mid n$ or $p \mid (n + (k - 1)d)$, we get an equation of the form (1.1). Then we apply Corollary 1 to find out all the exceptions. If $p \mid (n + i)$ where $i \neq 0, k - 1$, then we get an equation of the form (1.3). Now we apply Corollary 2 to find out all the exceptions. Thus Corollaries 1 and 2 can be combined to list all the solutions of (1.4) when $1 < d \leqslant 67$. If there exists no prime $\geqslant k$ dividing the left hand side of (1.1) to an odd power, then $(n, d, k) = (75, 23, 4)$ by Corollary 1. Thus we obtain all the finitely many triples $(n, d, k)$ with $1 < d \leqslant 67, k \geqslant 4$ and $\gcd(n, d) = 1$ such that there exists at most one prime $p \geqslant k$ dividing the left hand side of (1.1) to an odd power. The case $k = 3$ of the preceding assertion remains open.

As in Shorey and Tijdeman [16], the proofs depend on comparing an upper bound and lower bound for $n + (k - 1)d$. For example, in proving Theorem 1(ii) we show that (1.1) with $k - 1$ prime which we may assume by Lemma 16 implies

$$n + (k - 1)d \geqslant \tfrac{1}{2}k^3 + 3.25k^2 \quad \text{for } k \geqslant 104, \tag{1.5}$$

$$n + (k - 1)d < \min(\tfrac{1}{4}k^2d + (k - 1)d, k^3 + 4.25k^2), d < 4k \quad \text{for } k \geqslant 12 \tag{1.6}$$

and a sharper inequality

$$n + (k - 1)d < \min(\tfrac{1}{4}k^2d + (k - 1)d, \tfrac{1}{2}k^3 + 3.25k^2), d < 3k \quad \text{for } k \geqslant 68 \tag{1.7}$$

when $d$ is a power of an odd prime with $d \nmid n$. We combine (1.5) and (1.7) to conclude that $k < 104$. Then we apply an algorithm given in Section 9 to solve (1.1) for the

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

finite but large number of possibilities $(n, d, k)$ given by (1.6) for $12 \leqslant k < 68$ and (1.7) for $68 \leqslant k < 104$. See Lemma 12 for proofs of (1.6) and (1.7). An algorithm for (1.5) is given in Lemma 6 and it yields very sharp lower bounds as shown in Corollary 3. It is quite efficient and this is also the case with the algorithm of Section 9 mentioned above. These algorithms are new contributions in the proofs of our theorems. The inequality (1.6) is an explicit version of one essentially contained in [16] but the improvement (1.7) is new and useful for the proofs.

The approach of this paper works also for other values of $\chi$ but this may increase computational load considerably. This is why we have avoided taking $\chi = 11$ in our results. Further, if $d$ is divisible by more than one prime which are not fixed, then the method in Sections 7 and 8 would give $n < C_1k^3$ and $d < C_2k^2$ where $C_1, C_2$ are some effectively computable absolute constants. Also the bound for $k$ obtainable would be very large. In that case covering the remaining values of $k$ may become computationally impossible. Apart from the techniques of [3] and [16], the proofs involve developing a fundamental argument of Erdős given in Lemma 3 and its repeated applications leading to Corollary 3, an extensive use of Legendre Symbol and congruences, the method of Runge for the case $k = 8, b = 1, d = p^\alpha$ and several other arguments. The algorithms referred above are carried out by MATHEMATICA on a computer. We also use SIMATH for solving several elliptic equations. This package has already been used in [4] in a similar context but we use some combinatorial arguments to ensure that we get only those elliptic equations that can be solved by SIMATH. In the next section we continue listing the notation required in the paper and we also give a plan of the paper at the end of the section.

## 2. Notation

Unless otherwise specified, we shall always assume that $d \in \mathcal{D}$ where $\mathcal{D}$ is given by (1.2). We see that every $d \neq 30, 60, 70, 84, 90, 132$ can be uniquely written as $\chi\tau^\alpha$ with $\chi, \tau, \alpha$ satisfying (1.2) such that

$$\chi < \tau^\alpha \tag{2.1}$$

and we shall always represent $d \neq 30, 60, 70, 84, 90, 132$ in this way throughout the paper. Thus $\chi = 2$ if $d = 10$ and $\chi = 5$ if $d = 45$. By (2.1), we see that $\alpha \geqslant 2$ if $d = 3 \cdot 2^\alpha$; $\alpha \geqslant 3$ if $d = 5 \cdot 2^\alpha, 7 \cdot 2^\alpha$ and $\alpha \geqslant 4$ if $d = 9 \cdot 2^\alpha$. Further, we write $90 = 10p^2$ with $p = 3$; $30 = 6p$ and $60 = 12p$ with $p = 5$; $70 = 10p$ and $84 = 12p$ with $p = 7$; $132 = 12p$ with $p = 11$. Thus $\chi = 6$ if $d = 30$ and $\chi = 10$ if $d = 70, 90$ and $\chi = 12$ if $d = 60, 84, 132$. One may also take $30 = 10p$ with $p = 3$ and $\chi = 10$ but we use the earlier representation to avoid confusion. We denote by $\tau'$ a prime divisor of $d$. Thus $\tau'$ is either $\tau$ or a prime divisor of $\chi$. Further we put

$$\chi_1 = \begin{cases} \chi & \text{if } d = \chi p^\alpha, \\ 2\chi & \text{if } d = \chi 2^\alpha. \end{cases} \tag{2.2}$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Let $q_1 < q_2 < \cdots$ be the sequence of all primes coprime to $d$ and $p_1 < p_2 < \cdots$ be the sequence of all primes. We write $\pi_d(x)$ for the number of primes $\leqslant x$ and coprime to $d$, $\pi(x)$ for the number of primes $\leqslant x$. We shall use the estimates (see [9, p. 69])

$$q_i \geqslant p_i \geqslant i \log i \quad \text{for } i \geqslant 1, \tag{2.3}$$

$$\pi_d(x) \leqslant \pi(x) \leqslant \frac{x}{\log\, x} + \frac{1.5\, x}{\log^2 x} \quad \text{for } x > 1 \tag{2.4}$$

and

$$\pi(x) > \frac{x}{\log\, x} \quad \text{for } x > 17. \tag{2.5}$$

For an integer $x > 0$, we write

$$q_i(x) = q_{\pi_d(x)+i} \quad \text{with } i \geqslant 1 \tag{2.6}$$

and

$$\delta = \frac{n + (k-1)d}{k^3}. \tag{2.7}$$

Further we put

$$\beta = \beta(d, k) = \prod_{\tau' | d} \tau'^{-\mathrm{ord}_{\tau'}(k-1)!}, \qquad \beta_1 = \beta_1(d, k) = (k-1)!\beta$$

and for $s > 0$

$$\beta_2(s) = \beta_2(d, k, s) = k - 1 - \frac{(k-1)\log(k-1) + \log\beta}{2\log(k-1) + \log s - \log 2} - \pi_d(k-1) - 1, \tag{2.8}$$

$$\beta_3(s,h) = \beta_3(d,k,s,h) = \begin{cases} k - 1 - \frac{(k-1)\log(k-1)+\log\beta}{3\log k + \log(s - \frac{d}{k^2})} - \pi_d(k-1) - h, & \text{if } s > \frac{d}{k^2} + \frac{2}{k^3}, \\ 0, \quad \text{otherwise,} \end{cases}$$

and

$$\beta_4(s,h) = \beta_4(d,k,s,h) = k - 1 - \frac{(k-1)\log(k-1) + \log\beta}{3\log(k-1) + \log s - \log 2} - \pi_d(k-1) - 1 - h.$$

Now we set

$$F(s,h) = \begin{cases} \beta_3(s,h), & \text{if } d = p^\alpha, 4p^\alpha, \\ \beta_4(s,h), & \text{otherwise,} \end{cases}$$

and $F^*(s,h) = \max(1, [F(s,h)] + 1)$. For any $r > 0$ and $s > 0$, we put $N_1(r,s) = [(r + s - 1)/s]$ and for any prime $\tau'$ dividing $d$, we write

$$N_2(r,\tau',d)=\begin{cases} N_1(r,2), & \text{if } \tau'=2, 2\parallel d,\\ N_1(r,4), & \text{if } \tau'=2, 4\parallel d,\\ N_1(r,8), & \text{if } \tau'=2, 8\mid d,\\ \min(N_1(r,\tau')(\frac{\tau'-1}{2}),[r]), & \text{if } d \text{ is odd.}\end{cases}$$

For any integer $\mu > 0$, we denote by $d_1(\mu)$ the number of ways $\mu$ can be written as $\mu_1\mu_2$ such that $\gcd(\mu_1,\mu_2)=2$. For example if $\mu=16$, then $(\mu_1,\mu_2)\in\{(2,8),(8,2)\}$ and $d_1(16)=2$. For $r>0$, we define

$$G_1(r)=\sum_{\substack{\mu<r\\ 8\mid\mu}} d_1(\mu), \tag{2.9}$$

$$G_2(r)=\begin{cases} 0, & \text{if } 1<d\leqslant 4,\\ 1, & \text{if } 5\leqslant d\leqslant 8,\\ N_2(\frac{k}{r},2,d), & \text{if } d \text{ is even} >8,\\ N_2(\frac{k}{r},\tau',d), & \text{if } d \text{ is odd} >8, \tau'\mid\chi, \tau'\in\{3,5,7\},\\ [\frac{k}{r}]+G_1(r), & \text{if } d=p^\alpha\end{cases}$$

and

$$G_3=\begin{cases} 0, & \text{if } d\in\{2^\alpha,p^\alpha,2p^\alpha,3p^\alpha,4p^\alpha\}\\ 3, & \text{if } d\in\{5p^\alpha,7p^\alpha\}\\ 6, & \text{if } d\in\{6p^\alpha,8p^\alpha,9p^\alpha,10p^\alpha,3\cdot 2^\alpha\}\\ 9, & \text{if } d=12p^\alpha\\ 12, & \text{if } d=5\cdot 2^\alpha\\ 18, & \text{if } d=7\cdot 2^\alpha, 9\cdot 2^\alpha.\end{cases}$$

We put

$$G_4(r)=G_2(r)+G_3. \tag{2.10}$$

Let $d_1<\cdots<d_t$ be integers with $d_i\in[0,k)$ for $1\leqslant i\leqslant t$. Thus $t\leqslant k$. We shall always take $t=k$ or $t=k-1$ with $t\geqslant 3$. We consider the equation

$$(n+d_1d)\cdots(n+d_td)=by^2 \tag{2.11}$$

in positive integers $n,d,k,b,y$ and $d_1,\ldots,d_t$. We recall that $P(b)\leqslant k$. We shall always assume that $\gcd(n,d)=1$ whenever we refer to (2.11). This is not the case regarding (1.1) which will be referred only in Section 11. Thus $\gcd(n,d)=1$ throughout Sections 3–10. If $t=k$, we see that $d_i=i$ for $0\leqslant i<k$. If $t=k-1$, then the left-hand side of (2.11) is obtained by omitting a term $n+id$ for some $i$ with $0\leqslant i<k$ from $\{n,n+d,\ldots,n+(k-1)d\}$. Further (2.11) with $t=k-1$ includes (1.3). We shall assume that

$$(n,d,k)\notin\{(2,7,3),(1,5,4),(2,7,4),(3,5,4),(1,2,5),(2,7,5),(4,7,5),(4,23,5)\}. \tag{2.12}$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Then we see from [17] and [12, Theorem 4] that the left-hand side of (2.11) is divisible by a prime exceeding $k$. Furthermore, by [12, Theorem 4′], the left-hand side of (2.11) is divisible by at least two distinct primes exceeding $k$ whenever $t = k \geqslant 4$. Thus we see from (2.11), (2.6) and (2.7) that

$$n + (k-1)d \geqslant q_1^2(k) \geqslant (k+1)^2 \tag{2.13}$$

and

$$\delta \geqslant \frac{q_1^2(k)}{k^3} > \frac{1}{k}. \tag{2.14}$$

Further, by (2.11), we write

$$n + d_i d = a_i x_i^2,\ P(a_i) \leqslant \max(P(b), k-1),\ a_i \text{ square free for } 1 \leqslant i \leqslant t \tag{2.15}$$

and

$$n + d_i d = A_i X_i^2,\ P(A_i) \leqslant \max(P(b), k-1),\ \gcd\Big(\prod p, X_i\Big) = 1, \qquad \text{for } 1 \leqslant i \leqslant t, \tag{2.16}$$

where the product $\prod p$ is taken over all primes $p$ with $p \leqslant \max(P(b), k-1)$. Let $S = \{A_1, \ldots, A_t\}$, $S_1 = \{\mu \mid X_\mu \neq 1, 1 \leqslant \mu \leqslant t\}$ and $S_2$ be the set of all $A_\mu \in S$ with $\mu \in S_1$. We divide the set $S_1$ into subsets with the property that two integers $\mu, \nu$ with $1 \leqslant \mu, \nu \leqslant t$ belong to the same subset if and only if $A_\mu = A_\nu$. Now we arrange the integers in each subset in the increasing order. If $\mu_0$ is the maximum of the integers in a particular subset, we call the subset as $V_{\mu_0}$. Thus $S_1 = \cup V_{\mu_0}$. Let $S'$ be the set of such $\mu_0$'s. We put $S_1^{(i)} = \{\mu_0 \mid \mu_0 \in S', |V_{\mu_0}| = i\}$. Then we see that

$$|S_1| = \sum_{i \geqslant 1} i |S_1^{(i)}| \tag{2.17}$$

and

$$|S_2| = |S'| = \sum_{i \geqslant 1} |S_1^{(i)}|. \tag{2.18}$$

Analogously, we partition the set of $a_i$'s in the following way. Let $R = \{a_1, \ldots, a_t\}$ and $R_1 = \{i \mid 1 \leqslant i \leqslant t\}$. We divide $R_1$ into subsets with the property that two integers $\mu, \nu$ with $1 \leqslant \mu, \nu \leqslant t$ belong to the same subset if and only if $a_\mu = a_\nu$. We arrange the integers in each subset in the increasing order. If $\mu_0$ is the maximum of the integers in a particular subset, we call the subset as $W_{\mu_0}$. Thus $R_1 = \cup W_{\mu_0}$. Let $R'$ be the set of such $\mu_0$'s. We put $R_1^{(i)} = \{\mu_0 \mid \mu_0 \in R', |W_{\mu_0}| = i\}$. Then $|R| = |R'| = \sum_{i \geqslant 1} |R_1^{(i)}|$.

Let $B_1 < B_2 < \cdots < B_{|S|}$ and $e_1 < e_2 < \cdots < e_{|R|}$ be the distinct elements of $S$ and $R$, respectively. Suppose $\tau'$ is a prime and $\alpha' > 0$ is an integer such that $\tau'' = \tau'^{\alpha'}$ divides $d$. Then by (2.16), we see that $n \equiv A_i X_i^2 (\mathrm{mod}\ \tau'')$. If $X^2$ can take value in $\eta$ residue classes mod $\tau''$, then we find that all the $B_i$'s fall in $\eta$ residue classes mod $\tau''$. We write any integer $i \geqslant 1$ as $i = i_0\eta + i_1$ where $i_0, i_1$ are integers with

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

$0 < i_1 \leqslant \eta$. Then we observe that $B_i \geqslant i_0\tau'' + i_1$. Thus $B_i \geqslant (i\tau''/\eta) - (\tau'' - \eta)$. For instance, if $\tau'' = 3$, then $\eta = 1$ and $B_i \geqslant 3i - 2$. We can extend this argument to more than one prime power dividing $d$ by Chinese Remainder Theorem. Further, by (2.15), the above argument can be applied to $e_i$'s as well. We put

$$\tau_1 = \tau_1(d) = \begin{cases} d, & \text{if } d = 2, 4, 12, \\ \chi, & \text{if } d = \chi p^\alpha \text{ with } \chi \neq 9, \\ 8\chi, & \text{if } d = \chi 2^\alpha \text{ with } \alpha > 2, \chi \neq 9, \\ 3, & \text{if } d = 9p^\alpha, \\ 24, & \text{if } d = 9 \cdot 2^\alpha \end{cases}$$

and

$$u_d(i) = \begin{cases} \tau_1 i - \tau_1 + 1, & \text{if } d = \chi\tau^\alpha, \text{with } \chi \neq 5, 7, 10, \\ \max(\frac{\tau_1}{2} i - \tau_1 + 2, 1), & \text{if } d = 5\tau^\alpha, 10\tau^\alpha, \\ \max(\frac{\tau_1}{3} i - \tau_1 + 3, 1), & \text{if } d = 7\tau^\alpha. \end{cases} \tag{2.19}$$

By the argument given above, we see that

$$B_i \geqslant u_d(i) \quad \text{for } 1 \leqslant i \leqslant |S|; \quad e_i \geqslant u_d(i), \quad \text{for } 1 \leqslant i \leqslant |R|. \tag{2.20}$$

Let $d = h_1h_2$ with $\gcd(h_1, h_2) = 1$ or 2. We call such pairs $(h_1, h_2)$ as partitions of $d$. When $a_i = a_j$ with $i \neq j$ we observe from (2.15) that $(i - j)d = a_j(x_i^2 - x_j^2)$. Since $\gcd(n, d) = 1$, we have $\gcd(d, a_j) = 1$ and $\gcd(d, x_i - x_j, x_i + x_j) = 1$ or 2 according as $d$ is odd or even, respectively. Thus $d \mid (x_i^2 - x_j^2)$. We say that a partition $(h_1, h_2)$ of $d$ corresponds to $a_i = a_j$ with $i \neq j$ if $h_1 \mid (x_i - x_j)$ and $h_2 \mid (x_i + x_j)$. It is clear that such a partition $(h_1, h_2)$ of $d$ corresponding to $a_i = a_j$ with $i \neq j$ always exists. If $d$ is odd, we observe that it is unique. This need not be the case when $d$ is even. We define

$$M = \begin{cases} 0, & \text{if } d = 2, 4, \\ 1, & \text{if } d = p^\alpha, \\ 2, & \text{if } d = 2^\alpha, \text{with } \alpha > 2, 2p^\alpha, 3p^\alpha, 5p^\alpha, 7p^\alpha, 9p^\alpha, \\ 3, & \text{if } d = 4p^\alpha, \\ 4, & \text{if } d = 6p^\alpha, 8p^\alpha, 10p^\alpha, 3 \cdot 2^\alpha, 5 \cdot 2^\alpha, 7 \cdot 2^\alpha, 9 \cdot 2^\alpha, \\ 6, & \text{if } d = 12p^\alpha, \end{cases} \tag{2.21}$$

$$r_0 = \begin{cases} 4, & \text{if } 2 \parallel d, \\ 2, & \text{if } 4 \parallel d, \\ 1, & \text{if } 8 \mid d, \\ 8, & \text{if } d \text{ is odd and } d \neq p^\alpha, \\ 16, & \text{if } d = p^\alpha, \end{cases} \tag{2.22}$$

$$\epsilon_0 = \begin{cases} 2, & \text{if } d \text{ is even and } d/\chi_1 \text{ odd}, \\ 1, & \text{otherwise}, \end{cases} \tag{2.23}$$

$$\epsilon_1 = \begin{cases} 2, & \text{if } d = \chi 2^\alpha, \\ 1, & \text{otherwise} \end{cases} \tag{2.24}$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

and

$$\epsilon_2 = \begin{cases} 2, & \text{if } 4 \mid d, \\ 1, & \text{otherwise.} \end{cases} \tag{2.25}$$

For any integer $m \geqslant 1$, we denote by $f(m)$ the number of $e_i$'s composed of $q_1, \ldots, q_m$. Then

$$f(m) \geqslant |R| - \sum_{\mu \geqslant m+1} \left( \left[ \frac{k}{q_\mu} \right] + \varepsilon_\mu \right) =: f_0(m), \tag{2.26}$$

where $\varepsilon_\mu = 0$ if $q_\mu > k$ or $q_\mu \mid k$ and $\varepsilon_\mu = 1$ otherwise. Since $e_i$'s are square free, we observe that

$$f(m) \leqslant 2^m. \tag{2.27}$$

We shall follow the notation introduced in Sections 1 and 2 throughout the paper.

We end this section with a plan of the paper. Every section, other than 6, 10, 11, begins with the precise assumptions to be followed in that section. These assumptions will not be mentioned in the statements of lemmas of that section. Further, in each section, we give a brief introduction to the results proved in that section. Sections 3 to 10 are devoted to solving (2.11) which we assume in this paragraph. In Section 3 we solve (2.11) completely for $k \leqslant 11$ and $d \neq p^\alpha$. In the subsequent sections we solve (2.11) for other values of $d$ and $k$. In Section 4, we give a lower bound for the number of distinct $A_i$'s with $X_i \neq 1$ which leads to a lower bound for $n + (k-1)d$ in Section 5. The next step is to find an upper bound for $n + (k-1)d$ in Sections 7 and 8. To achieve this, we show in Section 6 that there are several $a_i$'s which are repeated. A comparison of the lower and upper bounds for $n + (k-1)d$ imply that $n, d, k$ are bounded as proved in Section 8. We give an algorithm in Section 9 to solve (2.11) when $n, d, k$ are bounded. In fact, we solve (2.11) in Section 9 with the assumption $k-1$ prime if $k \geqslant 12$ which we justify in the Section 10. The final Section 11 is devoted to the proofs of the theorems and corollaries.

## 3. Equation (2.11) with $\chi > 1$ and $k$ Small

We suppose (2.11) with either $P(b) \leqslant k$ if $t = k$ or $P(b) < k$ if $t = k-1$. In this section, we solve (2.11) with $d \neq p^\alpha$ and $k \leqslant 11$ by using Legendre symbol. We begin with

LEMMA 1. *Let $i$ be a nonnegative integer.*

(i) *Suppose $i < k-1$ and $n + id = x_i^2$, $n + (i+1)d = x_{i+1}^2$. Then*

$$(x_i, x_{i+1}) = \left( \frac{h_2 - h_1}{2}, \frac{h_2 + h_1}{2} \right)$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

*for some partition* $d = h_1h_2$ *with* $h_1 < h_2$ *of* $d$ *satisfying* $\gcd(h_1, h_2) = 1$ *if* $d$ *is odd and* $\gcd(h_1, h_2) = 2, 8 \mid d$ *if* $d$ *is even.*

(ii) *Suppose* $i < k - 2$ *and* $n + id = x_i^2, n + (i+2)d = x_{i+2}^2$. *Then* $d$ *is even and*

$$(x_i, x_{i+2}) = \left(\frac{h_2 - h_1}{2}, \frac{h_2 + h_1}{2}\right)$$

*where* $2d = h_1h_2$ *with* $h_1 < h_2$ *and* $\gcd(h_1, h_2) = 2$.

(iii) *Suppose* $i < k - 2$ *and*

$$n + id = x_i^2, n + (i+1)d = x_{i+1}^2, n + (i+2)d = x_{i+2}^2.$$

*Then* $(x_i, x_{i+1}, x_{i+2}) = (1, 5, 7)$.

(iv) *Suppose* $i < k - 3$ *and*

$$n + id = x_i^2, n + (i+2)d = x_{i+2}^2, n + (i+3)d = x_{i+3}^2.$$

*Then* $(x_i, x_{i+2}, x_{i+3}) \in \{(5, 11, 13), (1, 9, 11)\}$.

(v) *Suppose* $i < k - 3$ *and*

$$n + id = x_i^2, n + (i+1)d = x_{i+1}^2, n + (i+3)d = x_{i+3}^2.$$

*Then* $(x_i, x_{i+1}, x_{i+3}) = (1, 3, 5)$.

*Proof.* (i) Since $d = x_{i+1}^2 - x_i^2$, the assertion is immediate.

(ii) We have $2d = x_{i+2}^2 - x_i^2$ which implies that both $x_i, x_{i+2}$ are odd or even. Hence, $d$ is even. Now the assertion follows immediately.

(iii) We observe that $8 \mid d$ by (ii) and (i). Let $d = 8p^\alpha$. Then $(x_i, x_{i+1})$ and $(x_{i+1}, x_{i+2})$ belong to $\{(2p^\alpha - 1, 2p^\alpha + 1), (p^\alpha - 2, p^\alpha + 2)\}$ implying $d = 24$ which is not possible by (2.1). The proof for the other cases $d = \chi 2^\alpha$ with $\chi \in \{1, 3, 5, 7, 9\}, \alpha \geqslant 3$ is similar. The triple $(1, 5, 7)$ corresponds to $\chi = \alpha = 3$.

(iv) By (ii) and (i), we have $8 \mid d$. Let $d = 8p^\alpha$. Then $(x_i, x_{i+2}) \in \{(4p^\alpha - 1, 4p^\alpha + 1), (p^\alpha - 4, p^\alpha + 4)\}$ and $(x_{i+2}, x_{i+3}) \in \{(2p^\alpha - 1, 2p^\alpha + 1), (p^\alpha - 2, p^\alpha + 2)\}$. This implies $d = 40$ contradicting (2.1). Let $d = \chi 2^\alpha$ with $\chi \in \{1, 3, 5, 7, 9\}, \alpha \geqslant 3$. Then $(x_i, x_{i+2})$ equals $(\chi 2^{\alpha-1} - 1, \chi 2^{\alpha-1} + 1)$ or $(|2^{\alpha-1} - \chi|, 2^{\alpha-1} + \chi)$. Further, $(x_{i+2}, x_{i+3})$ equals $(\chi 2^{\alpha-2} - 1, \chi 2^{\alpha-2} + 1)$ or $(|2^{\alpha-2} - \chi|, 2^{\alpha-2} + \chi)$. Thus $(x_i, x_{i+2}, x_{i+3}) \in \{(5, 11, 13), (1, 9, 11)\}$.

(v) We proceed as in (iv) to get the assertion. □

LEMMA 2. *Let* $d \neq p^\alpha$ *and* $k \leqslant 11$. *Assume that* $k \geqslant 6$ *if* $t = k - 1$ *and* $d = 5p^\alpha, 7p^\alpha$. *If* $t = k$, *then either* $k = 3, d = 7p^\alpha$ *or* $(n, d, k) = (1, 24, 3)$. *If* $t = k - 1$, *then* $k = 4$ *and* $(n, d) \in \{(1, 8), (1, 24), (1, 40), (25, 48)\}$.

*Proof.* Let $k = 3$. Then $t = k$ since $t \geqslant 3$. Let $d$ be odd. If $3 \mid d$, we see from (2.15) and $\gcd(n, d) = 1$ that $a_i$'s belong to $\{1, 2\}$. Since $a_0x_0^2 \equiv a_1x_1^2 \equiv a_2x_2^2 \pmod{d}$, we have $(a_0/3) = (a_1/3) = (a_2/3)$. It follows that either $a_0 = a_1 = a_2 = 1$ or $a_0 = a_1 = a_2 = 2$. However, at most two of the numbers $n, n+d, n+2d$ can be even. This implies that $a_0 = a_1 = a_2 = 1$. Now the assertion follows from Lemma 1(iii).

Let $d = 5p^\alpha$ and $3 \nmid d$. Then $a_i$'s belong to $\{1, 6\}$ or $\{2, 3\}$. By Lemma 1(iii), we get $(a_0, a_1, a_2) \in \{(1, 1, 6), (1, 6, 1), (6, 1, 1), (2, 3, 2)\}$. Let $(a_0, a_1, a_2) = (1, 1, 6)$. Then $n + 2d \equiv 0 \pmod 3$. Hence, $1 = (x_0^2/3) = (n/3) = (-2d/3) = (d/3)$. But we also have $1 = (x_1^2/3) = ((n + d)/3) = (-d/3) = -(d/3)$, a contradiction. All other cases are excluded similarly by using Legendre Symbol mod 3. If $d$ is even, then $a_i$'s belong to $\{1, 3\}$ and we conclude as above that $(n, d) = (1, 24)$.

Let $k = 4$ and $t = k$. By the result of Euler stated in Section 1 and Lemma 1, we see that there are exactly 3 distinct $a_i$'s. On the other hand, we find that $a_i$'s belong to $\{1, 3\}$ if $d$ is even, $\{1, 2\}$ if $3 \mid d$, $\{1, 6\}$ or $\{2, 3\}$ if $5 \mid d$ and $\{1, 2\}$ or $\{3, 6\}$ if $7 \mid d$. This is not possible. Now let $t = k - 1$. Suppose that $d$ is even. We see that $a_i$'s take values from $\{1\}$ if $4 \mid d$ and from $\{1, 3\}$ if $2 \parallel d$. Let $4 \mid d$. We apply Lemma 1 to see that $(n, d) \in \{(1, 8), (1, 24), (1, 40), (25, 48)\}$. Let $2 \parallel d$. There are two $a_i$'s equal to 1 or 3. Thus for some $0 \leqslant j < i < 4$, we have

$$(i - j)d = a(x_i^2 - x_j^2) \tag{3.1}$$

with $a_i = a_j = a = 1$ or 3 and $x_i, x_j$ odd. The right-hand side of (3.1) is divisible by 8. This is a contradiction since $2 \parallel d$. Suppose $d$ is odd. Then $3 \mid d$ by the assumption and $a_i$'s belong to $\{1, 2\}$. Further, by Lemma 1, we find that one of the $a_i$'s must be equal to 2. Since 2 can divide at most two $a_i$'s, there is an $a_i$ equal to 1. Thus $-1 = (\frac{2}{3}) = (\frac{1}{3}) = 1$, a contradiction.

Let $k = 5$. Since 5 can divide at most one $a_i$, we omit from the left-hand side of (2.11) the term divisibile by 5 if $t = k$ and $P(b) = k$ to observe that there is no loss of generality in assuming that $P(b) < k$ whenever $d \neq 7p^\alpha$. Let $d$ be even. Now we argue as in the case $k = 4$ to assume that $2 \parallel d$ and $a_i$'s belong to $\{1, 3\}$. Since $t \geqslant 4$, there are two $a_i$'s equal to 1. Thus (3.1) is satisfied with $a = 1$ and $0 \leqslant j < i \leqslant 4$. Hence, $a_0 = a_4 = 1$. Further at least one of the remaining $a_i$'s equals 1 since no two of them can take the value 3. Now we apply again (3.1) to arrive at a contradiction. Let $d$ be odd. Suppose $3 \mid d$. Then $a_i = 1$ for all $i$ or $a_i = 2$ for all $i$. Since at most three $a_i$'s can take the value 2, the latter possibility is excluded and the former is excluded by Lemma 1. Let $5 \mid d$ and $3 \nmid d$. Then $t = k$ by the assumption. Further $a_i$'s belong to $\{1, 6\}$ or $\{2, 3\}$. The first possibility is excluded by Lemma 1 while the second possibility does not hold since 3 can divide at most two $a_i$ 's and the three other $a_i$'s cannot be equal to 2. Let $7 \mid d$ with 3 and 5 not dividing $d$. Then $t = k$ and $a_i$'s belong to $\{1, 2, 15, 30\}$ or $\{3, 5, 6, 10\}$. Since 5 divides at most one $a_i$ and 3 divides at most two $a_i$'s we see that the latter possibility does not hold. In the first possibility if there are three odd terms, then $(a_0, a_2, a_4) \in \{(1, 1, 1), (15, 1, 1), (1, 15, 1), (1, 1, 15)\}$ which is excluded by (3.1). Thus we may assume that there are exactly two odd terms and by (3.1), one of them has its $a_i = 15$ implying that $(d/5) = -1$. Further, we see from (3.1) that the $a_i$'s corresponding to the three even terms are $(a_0, a_2, a_4) = (2, 2, 1), (1, 2, 2), (1, 2, 1)$. Let $(a_0, a_2, a_4) = (2, 2, 1)$. If $a_1 = 15$, we see from $a_0 = a_2 = 2$ that $3 \mid d$, a contradiction. If $a_3 = 15$, then $a_4 = 1$ implies that $(d/5) = 1$, a contradiction. The other possibilities are excluded similarly.

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Let $k = 6$. First let $d$ be even. If $8 \mid d$, we observe that $a_i \in \{1\}$ contradicting Lemma 1. If $4 \parallel d$, we see that $a_i \in \{1, 5\}$ and there is an $i$ with $a_i = a_{i+1} = 1$ which is not possible by (3.1). Let $2 \parallel d$. From (3.1) we see that no other value of $a_i$ except 1 is repeated and exactly one of the relations $a_0 = a_4 = 1$ and $a_1 = a_5 = 1$ holds. Then at least three $a_i$'s must assume the values 3, 5, 15 which is not possible by (3.1). Let $d$ be odd. The argument for the cases $3 \mid d, 5 \mid d$ is similar to the case $k = 5$. Let $7 \mid d$. Then $a_i$'s belong to $\{1, 2, 15, 30\}$ or $\{3, 5, 6, 10\}$. Arguing as earlier, we need to consider only $t = k - 1$, $a_i$'s belong to $\{1, 2, 15\}$, 15 equals an $a_i$ corresponding to an odd term and an odd term is omitted. Then we see from (3.1) that the $a_i$'s corresponding to the three even terms $\{a_0, a_2, a_4\}$ or $\{a_1, a_3, a_5\}$ belongs to $\{(2, 2, 1), (1, 2, 2), (1, 2, 1)\}$. Let us take the even terms to be $n, n + 2d, n + 4d$. Then we observe that $n + 2d \equiv 2 \pmod 8$. Let $(a_0, a_2, a_4) = (2, 2, 1)$. Suppose $15 \mid (n + d)$. If $n + 5d$ is not an omitted term, then $(n/5) = ((n + 5d)/5) = (x_5^2/5) = 1$. On the other hand, $(n/5) = (2x_0^2/5) = -1$. This is a contradiction implying that $n + 5d$ is the omitted term. Thus $n + 3d \equiv 1 \pmod 8$ which, together with $n + 2d \equiv 2 \pmod 8$, implies that $d \equiv 7 \pmod 8$. Also $n + d \equiv 7 \pmod 8$ which, together with $n + 2d \equiv 2 \pmod 8$, gives $d \equiv 3 \pmod 8$, a contradiction. Thus $15 \nmid (n + d)$. The proof for the assertion $15 \nmid (n + 5d)$ is similar. Let $15 \mid (n + 3d)$. Then $-1 = (2x_2^2/5) = ((n + 2d)/5) = (4d/5)$ implying $(d/5) = -1$. On the other hand, $-1 = (2x_0^2/5) = (n/5) = (-3d/5) = (2d/5)$ implying $(d/5) = 1$, a contradiction. The other cases are excluded similarly. The possibility that $n + d, n + 3d, n + 5d$ are even is also excluded likewise.

Let $k = 7$. If $P(b) < 7$, the assertion follows from the case $k = 6$. If $P(b) = 7$, then $t = k$ by assumption and we omit the term divisible by 7 on the left hand side of (2.11) to observe that the assertion follows from $k = 6$.

Let $k = 8$. Then $t \geqslant 7$. Let $d$ be even. Suppose $8 \mid d$. Then $a_i \in \{1, 105\}$. Hence, there are at least six $a_i$'s equal to 1 and we use Lemma 1 to exclude this case. Let $4 \parallel d$. Then $a_i \in \{1, 5, 21, 105\}$ and there are at least four $a_i$'s equal to 1. Hence by (3.1), we see that either $a_0 = a_2 = a_4 = a_6 = 1$ or $a_1 = a_3 = a_5 = a_7 = 1$. Then 5, 105 is assumed by at most one $a_i$. Thus there are at least five $a_i$'s equal to 1 which is impossible by (3.1). Let $2 \parallel d$. Then $a_i \in \{1, 3, 5, 7, 15, 21, 35, 105\}$. If 7 divides two $a_i$'s, then the assertion follows from the case $k = 6$. Therefore there are at most three $a_i$'s divisible by 5 and 7. Further, by (3.1), we observe that $a_i = 3$ at most once only. Hence there are at least three $a_i$'s $\in \{1\}$ which is again not possible by (3.1). Let now $d$ be odd. There are at least 3 odd terms. If $3 \mid d$, then $a_i \in \{1, 7, 10, 70\}$ or $a_i \in \{2, 5, 14, 35\}$. Thus there are at least two odd terms with the same $a_i$ in $\{1, 7\}$ or $\{5, 35\}$ contradicting (3.1). The cases $5 \mid d$ and $7 \mid d$ follow similarly by considering Legendre Symbol mod 5 and mod 7, respectively.

The cases $k = 9, 10, 11$ follow from the case $k = 8$. □

## 4. Lower Estimate for the Number of $A_i$'s With $X_i \neq 1$

We assume (2.11) with $P(b) < k$. We determine explicitly a lower estimate for the number of $A_i$'s with $X_i \neq 1$. In other words, we estimate $|S_2|$ from below. This is

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

done in Lemma 5. This estimate has been derived from Lemmas 3, 4 and (4.7). Further, we remark that the proofs of Lemmas 3,4 and (4.7) can be adapted for any $d$ to get a lower bound for $|S_2|$. But the lower bound would be trivial when $\omega(d)$ is large.

LEMMA 3. *Let* $k \geqslant 4$. *Then*

$$|S_1| > t - \frac{(k-1)\log(k-1) + \log\beta}{\log d + \log(k-1)} - \pi_d(k-1) - 1 \tag{4.1}$$

*and*

$$|S_1| > t - \frac{(k-1)\log(k-1) + \log\beta}{\log n_0} - \pi_d(k-1) - \theta, \tag{4.2}$$

*where* $n_0 = \max(n, 3)$, $\theta = 1$ *if* $n = 1, 2$ *and* $\theta = 0$ *if* $n > 2$.

*Proof.* Let $S_3 = \{\mu \mid X_\mu = 1, 1 \leqslant \mu \leqslant t\}$ so that $|S_1| = t - |S_3|$. We may assume that $|S_3| > \pi_d(k-1)$ for a proof of (4.1). We follow an argument of Erdős. Let $q$ be a prime $<k$ with $q \nmid d$. Let $\mu_q$ be chosen such that

$$\mathrm{ord}_q(A_{\mu_q}) = \max_{i \in S_3} (\mathrm{ord}_q A_i).$$

Let $S_4$ be the subset of $S_3$ obtained by deleting $\mu_q$ for every such prime $q$. Thus $|S_4| \geqslant |S_3| - \pi_d(k-1)$. Let $\mu \in S_4$. Then $n + d_\mu d = A_\mu$ and

$$\mathrm{ord}_q(n + d_\mu d) \leqslant \mathrm{ord}_q(|d_\mu - d_{\mu_q}|),$$

since $\gcd(n, d) = 1$. Therefore

$$\mathrm{ord}_q\left(\prod_{\mu \in S_4} (n + d_\mu d)\right) \leqslant \mathrm{ord}_q(d_{\mu_q}!(k-1-d_{\mu_q})!) \leqslant \mathrm{ord}_q(k-1)!.$$

Thus

$$\prod_{\mu \in S_4} (n + d_\mu d) = \prod_{\substack{q \nmid d \\ q < k}} q^{\mathrm{ord}_q(\prod_{\mu \in S_4} (n + d_\mu d))} \leqslant \frac{(k-1)!}{\prod_{\tau' | d} \tau'^{\mathrm{ord}_{\tau'}(k-1)!}} = \beta_1.$$

This implies that $d^{|S_3| - \pi_d(k-1) - 1}(|S_3| - \pi_d(k-1) - 1)! \leqslant \beta_1$ and

$$n^{|S_3| - \pi_d(k-1)} \leqslant \beta_1. \tag{4.3}$$

We get

$$\begin{aligned}(|S_3| - \pi_d(k-1) - 1)\log d &\leqslant \log((k-1)\cdots(|S_3| - \pi_d(k-1))) + \log\beta \\ &< (k - |S_3| + \pi_d(k-1))\log(k-1) + \log\beta,\end{aligned}$$

the latter relation holds with strict inequality since $|S_3| \leqslant k-2$ for $k \geqslant 4$ as pointed out after (2.12). This shows that

$$|S_3| < \frac{(k-1)\log(k-1) + \log\beta}{\log d + \log(k-1)} + \pi_d(k-1) + \frac{\log d + \log(k-1)}{\log d + \log(k-1)}$$

which implies (4.1). By (4.3), we have

$$|S_3| < \frac{(k-1)\log(k-1) + \log\beta}{\log n} + \pi_d(k-1)$$

which yields (4.2) whenever $n \geqslant 3$. Let $n = 1, 2$. We see that $n + d_\mu d \geqslant 3$ for $\mu \in S_4$ except for at most one $\mu$ for which $d_\mu = 0$. Hence

$$n_0^{|S_3| - \pi_d(k-1) - 1} \leqslant \beta_1$$

implying (4.2) as above. $\square$

Let $r_0$ be given by (2.22) in the next three lemmas.

LEMMA 4. *For* $k \geqslant \max(r_0, 4)$ *we have* $|S_1^{(2)}| \leqslant G_2(r_0)$.

*Proof.* Let $\mu_0 \in S_1^{(2)}$. Then there exists $\mu_1 \in S_1$ with $\mu_0 > \mu_1$ such that $A_{\mu_0} = A_{\mu_1}$ and hence by (2.16), we have

$$(\mu_0 - \mu_1)d = A_{\mu_0}(X_{\mu_0} - X_{\mu_1})(X_{\mu_0} + X_{\mu_1}). \tag{4.4}$$

The left-hand side of (4.4) is less than $kd$ whereas the right-hand side is at least $4k$ since $X_{\mu_0} > k$ and $X_{\mu_1} > k$ are odd integers. Thus we see that $d > 4$. If $5 \leqslant d \leqslant 8$, then $A_{\mu_0} = 1$ implying $|S_1^{(2)}| = 1$. Now we assume that $d > 8$. Let $d$ be odd and $\tau'$ be a prime dividing $d$. Then by (2.16), we have

$$\left(\frac{A_j}{\tau'}\right) = \left(\frac{n}{\tau'}\right), \quad \text{for } 1 \leqslant j \leqslant t.$$

Further we observe that there are $(\tau' - 1)/2$ quadratic residues and $(\tau' - 1)/2$ quadratic nonresidues mod $\tau'$. Therefore the number of distinct $A_j \leqslant k/r_0$ does not exceed $N_2(k/r_0, \tau', d) \leqslant [k/r_0]$. Let $d$ be even. Then the number of distinct $A_j \leqslant k/r_0$ does not exceed $N_2(k/r_0, 2, d)$ since $A_j$'s are odd, $A_j \equiv n \pmod 4$ if $4 \mid d$ and $A_j \equiv n \pmod 8$ if $8 \mid d$. Therefore the number of distinct $A_{\mu_0} \leqslant k/r_0$ does not exceed $N_2(k/r_0, \tau', d)$. Let now $S_1^{(2)}(k/r_0) = \{\mu_0 \mid \mu_0 \in S_1^{(2)}$ and $A_{\mu_0} > k/r_0\}$. Then it is enough to show that

$$\left|S_1^{(2)}\left(\frac{k}{r_0}\right)\right| \leqslant G_1(r_0) \quad \text{if } d = p^\alpha \tag{4.5}$$

and $S_1^{(2)}(k/r_0) = \phi$ otherwise. To show this we proceed as follows. Let $d$ be written as $h_1 h_2$ with $h_1 \mid (X_{\mu_0} - X_{\mu_1})$ and $h_2 \mid (X_{\mu_0} + X_{\mu_1})$ and $\gcd(h_1, h_2) = 1$ or $2$. Thus (4.4) gives

$$k > \mu_0 - \mu_1 = A_{\mu_0}\left(\frac{X_{\mu_0} - X_{\mu_1}}{h_1}\right)\left(\frac{X_{\mu_0} + X_{\mu_1}}{h_2}\right).$$

Thus

$$\left(\frac{X_{\mu_0}-X_{\mu_1}}{h_1}\right)\left(\frac{X_{\mu_0}+X_{\mu_1}}{h_2}\right)<r_0, \tag{4.6}$$

since $A_{\mu_0}>k/r_0$. We write

$$\frac{X_{\mu_0}-X_{\mu_1}}{h_1}=r_1, \qquad \frac{X_{\mu_0}+X_{\mu_1}}{h_2}=r_2 \quad \text{with } r_1\,r_2=r'<r_0.$$

Then we observe that $4\mid r'$ if $2\parallel d$, $2\mid r'$ if $4\parallel d$. Also if $d$ is odd, then $\gcd(r_1,r_2)=2$ and $8\mid r'$. Hence by the choice of $r_0$, we may assume that $d=p^\alpha$. This implies, by (4.4), that $h_1=1, h_2=d$ and we see that the number of $(X_{\mu_0},X_{\mu_1})$ satisfying (4.6) is at most $G_1(r_0)$ by (2.9). This proves (4.5). □

LEMMA 5. *For* $k\geqslant\max(r_0,4)$ *we have* $|S_2|\geqslant|S_1|-G_4(r_0)$.

*Proof*. By subtracting (2.18) from (2.17), we see from Lemma 4 and (2.10) that it suffices to show

$$\sum_{i\geqslant 3}(i-1)|S_1^{(i)}|\leqslant G_3. \tag{4.7}$$

We denote by $\mu_0^*$ an element of $\cup_{i\geqslant 3}S_1^{(i)}$ for which $A_{\mu_0^*}=1$. It may or may not exist. Suppose $\mu_0\in\cup_{i\geqslant 3}S_1^{(i)}$. Then, $\mu_0\in S_1^{(i)}$ for some $i\geqslant 3$. Thus there exist $\mu_1,\dots,\mu_{i-1}$ with $\mu_0>\mu_1>\cdots>\mu_{i-1}$ such that $A_{\mu_0}=A_{\mu_1}=\cdots=A_{\mu_{i-1}}$. Hence,

$$(\mu-\nu)d=A_\mu(X_\mu-X_\nu)(X_\mu+X_\nu) \quad \text{for } \mu,\nu\in\{\mu_0,\dots,\mu_{i-1}\}, \mu>\nu. \tag{4.8}$$

Thus, $d>4$. We write $d=h_1h_2$ with $\gcd(h_1,h_2)=1$ or 2 such that $h_1\mid(X_\mu-X_\nu)$, $h_2\mid(X_\mu+X_\nu)$. Since $i\geqslant 3$, we see that (4.8) holds with

$$(\mu,\nu)\in\{(\mu_0,\mu_1),(\mu_0,\mu_2),(\mu_1,\mu_2)\}. \tag{4.9}$$

Let $U$ be the set of possible values of $h_1$. We consider (4.8) with $\mu=\mu_0$. If $i\geqslant|U|+2$, then there is a value of $h_1$ which divides $X_{\mu_0}-X_\nu$ for two distinct values of $\nu\in\{\mu_1,\dots,\mu_{i-1}\}$. For simplicity, we assume that $\nu=\mu_1$ and$\mu_2$. Thus $h_1$ divides $X_{\mu_0}-X_{\mu_1}$ and $X_{\mu_0}-X_{\mu_2}$ giving $h_1\mid(X_{\mu_1}-X_{\mu_2})$. We also have $h_2$ dividing $X_{\mu_0}+X_{\mu_1}$ and $X_{\mu_0}+X_{\mu_2}$. Therefore $h_2\mid(X_{\mu_1}-X_{\mu_2})$. Hence $X_{\mu_1}-X_{\mu_2}\geqslant d/2$. This is impossible by (4.8) with $\mu=\mu_1$ and $\nu=\mu_2$. Thus we conclude that $i\leqslant|U|+1$ which implies that

$$\sum_{i\geqslant 3}(i-1)|S_1^{(i)}|\leqslant|U|\sum_{i\geqslant 3}|S_1^{(i)}|. \tag{4.10}$$

Suppose $d\in\{2^\alpha,p^\alpha,2p^\alpha,3p^\alpha,4p^\alpha\}$. Then we have $U$ as $\{1\}$ if $d=p^\alpha$; $\{1,2\}$ if $d=2^\alpha$ or if $d=2p^\alpha$; $\{1,3\}$if $d=3p^\alpha$; $\{1,2,4\}$ if $d=4p^\alpha$. Suppose $d=2^\alpha$. Then $h_1\in\{1,2\}$ divides $X_{\mu_0}-X_{\mu_1}$ and $X_{\mu_0}-X_{\mu_2}$. Then $2^{\alpha-1}=\frac{d}{2}$ divides $X_{\mu_1}-X_{\mu_2}$. This is impossible by (4.8). Similarly $d\neq p^\alpha,2p^\alpha,3p^\alpha,4p^\alpha$ by (4.8). Thus $|S_1^{(i)}|=0$ for $i\geqslant 3$

and (4.7) follows. Now we consider the remaining values of $d$ other than $9p^\alpha, 5\cdot 2^\alpha, 7\cdot 2^\alpha$ and $9\cdot 2^\alpha$. Suppose $\mu_0 \neq \mu_0^*$. Then we see from (4.8) that there exists $(\mu, \nu)$ as given in (4.9) with $X_\mu - X_\nu \geqslant 2p^\alpha$ if $d \neq 3\cdot 2^\alpha$ and $X_\mu - X_\nu \geqslant 2^{\alpha-1}$ if $d = 3\cdot 2^\alpha$. This is impossible by (4.8) since $A_{\mu_0} \geqslant 2$ and further $A_{\mu_0} \geqslant 3$ if $d$ is even. Thus, $\mu_0 = \mu_0^*$ in these cases. Hence, we derive that $\sum_{i\geqslant 3}|S_1^{(i)}| = 1$ which together with (4.10) and $|U| = 3$ if $d = 5p^\alpha, 7p^\alpha$; $|U| = 6$ if $d = 6p^\alpha, 8p^\alpha, 10p^\alpha, 3\cdot 2^\alpha$; $|U| = 9$ if $d = 12p^\alpha$ implies (4.7). Finally we consider the cases $d = 9p^\alpha, 5\cdot 2^\alpha, 7\cdot 2^\alpha, 9\cdot 2^\alpha$. We argue as above to conclude that $A_{\mu_0}$ belongs to $\{1, 2\}$ if $d = 9p^\alpha$; $\{1, 3\}$ if $d = 5\cdot 2^\alpha$; $\{1, 3, 5\}$ if $d = 7\cdot 2^\alpha$; $\{1, 5, 7\}$ if $d = 9\cdot 2^\alpha$. Now the assertion (4.7) follows from (4.10) and $|U| = 3$ if $d = 9p^\alpha$; $|U| = 6$ otherwise. □

## 5. Iterative Procedure for Obtaining a Lower Estimate for $n + (k-1)d$

We assume (2.11) with $P(b) < k$. It is proved in Shorey and Tijdeman [16, Lemma 1] that for any $d$, we get $n + (k-1)d \geqslant C_3\, k^3 \log^2 k$ where $C_3$ is an absolute constant. But $C_3$ is not explicitly given and it turns out to be small. Therefore, it does not provide a good lower bound when $k$ is bounded. We show that it is possible to obtain a good lower bound for $n + (k-1)d$ whenever $d \in \mathcal{D}$, see Corollary 3. We shall derive Corollary 3 from Lemma 6 which involves an iterative procedure. This procedure makes use of the lower estimate for $|S_2|$ obtained in Lemma 5.

LEMMA 6. *Let $k \geqslant \max(r_0, 4)$. Then the following assertions hold.*

(i) $n + (k-1)d \geqslant u_d(\max([\beta_2(1) - G_4(r_0)] + 1, 1)p^2_{\pi(k-1)+1} =: fk^3$ *where $u_d(i)$ is given by* (2.19).

(ii) *Let $n + (k-1)d \geqslant g_1 k^3$ with $g_1 \geqslant \frac{1}{k}$. For $i \geqslant 2$, define $g_i$ by the recurrence relation*

$$g_i k^3 = u_d([F^*(g_{i-1}, G_4(r_0))])p^2_{\pi(k-1)+1}.$$

*Then $n + (k-1)d \geqslant g_i k^3$.*

(iii) *Let $i_0$ be fixed with $n + (k-1)d \geqslant g_{i_0}k^3$. Let*

$$h' = \frac{F^*(g_{i_0}, G_4(r_0))}{k}, \quad h'' = \begin{cases} .16, & \text{if } h' > 16, \\ \frac{h'}{2}, & \text{otherwise} \end{cases}$$

$$h_1' = h', \quad h_1'' = (h_1' - h'')k - 1 + \frac{k-1}{\log(k-1)}$$

*and*

$$\ell_1 = \frac{u_d([h''k] + 1)p^2_{[h_1'k] - [h''k] + \pi(k-1)}}{k^3}, \qquad \ell_1' = \frac{u_d(h''k)(h_1'' \log h_1'')^2}{k^3}.$$

*Then $n + (k-1)d \geqslant L_1 k^3$ and for $k \geqslant 19$, we have $n + (k-1)d \geqslant L_1' k^3$ where $L_1 = \max(g_{i_0}, \ell_1)$ and $L_1' = \max(g_{i_0}, \ell_1')$.*

(iv) *For* $i \geqslant 2$, *let*

$$h_i' = \frac{F^*(L_{i-1}, G_4(r_0))}{k}, \quad h_i'' = (h_i' - h'')k - 1 + \frac{k-1}{\log(k-1)}$$

*and*

$$\ell_i = \frac{u_d([h''k]+1)p^2_{[h_i'k]-[h''k]+\pi(k-1)}}{k^3}, \qquad \ell_i' = \frac{u_d(h''k)(h_i'' \log h_i'')^2}{k^3}.$$

*Then* $n+(k-1)d \geqslant L_i k^3$ *and for* $k \geqslant 19$, *we have* $n+(k-1)d \geqslant L_i' k^3$ *where* $L_i = \max(L_{i-1}, \ell_i)$ *and* $L_i' = \max(L_{i-1}', \ell_i')$.

*Proof.* We recall that $t \geqslant k-1$.

(i) Suppose $d \geqslant (k-1)/2$. Then we use (4.1) to estimate $|S_1|$. If $d < (k-1)/2$, we use (2.13) to find that $n > k^2/2$ which we use in (4.2) to estimate $|S_1|$. Thus we get $|S_1| > \beta_2(1)$ by (2.8). By Lemma 5, we have $|S_2| \geqslant [\beta_2(1) - G_4(r_0)] + 1$ and we recall that $|S_2| \geqslant 1$. Thus there are at least $\max([\beta_2(1) - G_4(r_0)] + 1, 1)$ distinct $A_j$'s with $j \in S_1$. We arrange the $A_j$'s in the increasing order and observe that each of the corresponding $X_j$'s has a prime factor $\geqslant k$. This yields the estimate in (i) by (2.20).

(ii) Let $n+(k-1)d \geqslant g_1 k^3$ and we prove the assertion for $i=2$. Let $d = p^\alpha, 4p^\alpha$. In these cases we proceed as follows. We may assume that $g_1 > d/k^2 + 2/k^3$ otherwise $F^*(g_1, G_4(r_0)) = 1$ and the assertion follows immediately from (2.13). Thus $n > (g_1 - d/k^2)k^3 > 2$. Now by (4.2) and Lemma 5, we get $|S_2| > \beta_3(g_1, G_4(r_0))$ which gives $n+(k-1)d \geqslant g_2 k^3$. Now let $d \notin \{p^\alpha, 4p^\alpha\}$. We use (4.1) if $d \geqslant (g_1(k-1)^2)/2$ and if otherwise, we use (4.2) to estimate $|S_1|$ and we apply Lemma 5. We derive that $|S_2| > \beta_4(g_1, G_4(r_0))$ which implies $n+(k-1)d \geqslant g_2 k^3$. The assertion for $i \geqslant 3$ follows similarly.

(iii) We have $n+(k-1)d \geqslant g_{i_0} k^3$. We proceed as in (ii) to get $|S_2| \geqslant F^*(g_{i_0}, G_4(r_0))$. Thus there are at least $[h_1'k]$ distinct $A_j$'s with $j \in S_1$. We arrange them in increasing order and remove the first $[h''k]$ of these $A_j$'s. Then we are left with $[h_1'k] - [h''k] > 0$ number of $A_j$'s each of which exceeds $u_d([h''k]+1)$ by (2.20). Now we arrange the corresponding $X_j$'s in the increasing order. Thus the largest $X_j$ is divisible by a prime $\geqslant p_{[h_1'k]-[h''k]+\pi(k-1)}$. This gives the first assertion. The second assertion follows by using (2.3) and (2.5) in the definition of $\ell_1$.

(iv) We proceed by induction on $i \geqslant 2$. We have $n+(k-1)d \geqslant L_1 k^3$. Hence, we get $|S_2| \geqslant F^*(L_1, G_4(r_0))$. Thus there are at least $[h_2'k]$ distinct $A_j$'s with $j \in S_1$. Further we observe that $F^*(s,h)$ is an increasing function of $s$. Hence $h_2' \geqslant h_1'$. Now we proceed as in (iii) to get $n+(k-1)d \geqslant u_d([h''k]+1)p^2_{[h_2'k]-[h''k]+\pi(k-1)}$. Hence, $n+(k-1)d \geqslant \max(L_1, \ell_2)k^3$. This proves the first assertion with $i=2$ and the second assertion follows by using (2.3) and (2.5) in the definition of $\ell_2$. The assertion for $i \geqslant 3$ follows similarly. □

*Table I.*

| $d$ | $v_1$ | $v_2$ | $v_2'$ |
|---|---|---|---|
| $p^\alpha$ | $\frac{1}{2}+\frac{13}{4k}$ | 104 | 318 |
| $2p^\alpha$ | $\frac{1}{2}+\frac{13}{2k}$ | 48 | 180 |
| $3p^\alpha$ | $\frac{1}{2}+\frac{39}{4k}$ | 30 | 80 |
| $4p^\alpha$ | $2+\frac{13}{k}$ | 80 | 308 |
| $5p^\alpha$ | $\frac{1}{2}+\frac{65}{4k}$ | 60 | 138 |
| $6p^\alpha$ | $\frac{1}{2}+\frac{39}{2k}$ | 42 | 98 |
| $7p^\alpha$ | $\frac{1}{2}+\frac{91}{4k}$ | 80 | 168 |
| $8p^\alpha$ | $2+\frac{26}{k}$ | 90 | 192 |
| $9p^\alpha$ | $\frac{1}{2}+\frac{117}{4k}$ | 68 | 132 |
| $9p^\alpha$ | $\frac{405}{4k}$ | 80 | 138 |
| $10p^\alpha$ | $\frac{1}{2}+\frac{65}{2k}$ | 54 | 128 |
| $12p^\alpha$ | $2+\frac{39}{k}$ | 60 | 132 |
| $2^\alpha$ | $2+\frac{13}{k}$ | 38 | 140 |
| $3\cdot 2^\alpha$ | $2+\frac{39}{k}$ | 60 | 300 |
| $5\cdot 2^\alpha$ | $2+\frac{65}{k}$ | 68 | 128 |
| $7\cdot 2^\alpha$ | $2+\frac{91}{k}$ | 102 | 174 |
| $9\cdot 2^\alpha$ | $2+\frac{117}{k}$ | 80 | 140 |
| $9\cdot 2^\alpha$ | $\frac{405}{k}$ | 90 | 140 |

COROLLARY 3. *Let $k-1$ be prime and $d \neq 2, 4$. Assume that $d \leqslant 3(k-1)$ if $d = p^\alpha$ and $d \leqslant 12(k-1)$ if $d = 4p^\alpha$. For $v_1, v_2$ given in* Table 1 *above we have $\delta \geqslant v_1$ for $k \geqslant v_2$.*

We use the exact values of $\pi(k)$ for the assertion of Corollary 3 with $v_2 \leqslant k < v_2'$. In fact the assumption $k-1$ prime is not used for $k \geqslant v'_2$.

*Proof.* We give proofs for the cases $d = p^\alpha$ and $d = 5p^\alpha$. The proofs for other cases are similar. We follow the notation of Lemma 6.

Let $d = p^\alpha$ and $d \leqslant 3(k-1)$. Then $r_0 = 16$. First, let $k \geqslant 318$. By Lemma 6(i), we get $f \geqslant .0888$. We put $g_1 = .0888$ and apply the iteration process in Lemma 6(ii) to obtain $g_2 \geqslant .1615, g_3 \geqslant .1697, g_4 \geqslant .1704$. We fix $i_0 = 4$. Then $g_{i_0} = .1704, h_1' \geqslant .3385, h'' = .16, \ell_1' \geqslant .4307$ and $L_1' \geqslant .4307$. Further $L_2' \geqslant .4987, L_3' \geqslant .5090, L_4' \geqslant .5105$. Thus by Lemma 6(iv), we have $\delta \geqslant .5105 \geqslant \frac{1}{2} + 13/(4k)$ for $k \geqslant 318$. Now we take

$104 \leqslant k < 318$. For these values of $k$, we use the exact value of $\pi(k)$ in Lemma 6. We give the details of computation for $k = 104$. By Lemma 6(i) we find that $f \geqslant .1221$. Now we take $g_1 = .1221$ and use the iteration process in Lemma 6 (ii) to get $g_2 \geqslant .2748, g_3 \geqslant .3053, g_4 \geqslant .3155$. We fix $i_0 = 4$. Then $g_{i_0} \geqslant .3155$, $h_1' \geqslant .2980, h'' = .16$ and $l_1 \geqslant .4951$. Hence $L_1 \geqslant .4951$. Now we use the iteration process in Lemma 6(iv) to compute $L_2 \geqslant .5513, L_3 \geqslant .5629, L_4 \geqslant .5629$. Thus we get $\delta \geqslant .5629 \geqslant \frac{1}{2} + 13/(4k)$ for $k = 104$. Similarly for $104 < k < 318$ with $k-1$ prime, we find $\delta \geqslant \frac{1}{2} + 13/(4k)$. This proves Corollary 3 when $d = p^\alpha$.

Let $d = 5p^\alpha$. Then $r_0 = 8$. Suppose $k \geqslant 138$. By Lemma 6(i), we get $f \geqslant .1658$. We take $g_1 = .1658$ and apply Lemma 6(ii) to secure $g_2 \geqslant .3217, g_3 \geqslant .3450, g_4 \geqslant .3474$. Let $i_0 = 4$. Then $g_{i_0} = .3474, h_1' \geqslant .2902, h'' = .16, \ell_1' \geqslant .5771$ and $L_1' \geqslant .5771$. Also $L_2' \geqslant .6375$. Thus by Lemma 6(iv), we have $\delta \geqslant .6375 \geqslant \frac{1}{2} + 65/(4k)$ for $k \geqslant 138$. Let $60 \leqslant k < 138$ and we fix $k = 60$. We derive from Lemma 6 that $g_1 = f \geqslant .2067, g_2 \geqslant .5081, g_3 \geqslant .5943$, $g_{i_0} = g_4 \geqslant .6373, h_1' \geqslant .2666, h'' = .16, \ell_1' \geqslant .8067$ and $L_1' \geqslant .8067$. Hence $\delta \geqslant .8067 \geqslant \frac{1}{2} + 65/(4k)$ for $k = 60$. Similarly the assertion follows for $60 < k < 138$ with $k-1$ prime. This proves Corollary 3 for $d = 5p^\alpha$. □

## 6. An Upper Bound for the Number of Distinct $a_i$'s

We show that not all $a_i$'s are distinct. For example, we prove that $|R| < k-1$ whenever (2.11) with $t = k$ and $b = 1$ holds. We achieve this in two stages viz., when $k < 12$ and when $k \geqslant 12$. First when $k < 12$, by Lemma 2 we need to consider only the case $d = p^\alpha$. This is done in Lemma 7 below where we may assume that $k \geqslant 6$ by the results of Fermat and Obláth stated in Section 1. As in Lemma 2, here again we make use of Legendre Symbol. Further we resort to Runge's method for the case $k = 8$. Secondly for $k \geqslant 12$, the method rests on an argument of Erdős and Rigge as explained in Lemma 8 below and we prove a sharper inequality than $|R| < k-1$ which is also valid when $t = k-1$ or $b > 1$. Further the arguments of Lemma 8 have been applied in Lemma 8′ to exclude the cases $d = 2, 4$. The proof of Lemma 8 extends to any $d$ and bounded $M$. In that case, the upper bounds for $|R|$ in Lemma 8 are valid whenever $k$ exceeds a number depending only on $M$.

LEMMA 7. *Let* $d = p^\alpha$ *and* $6 \leqslant k \leqslant 11$. *Assume that* $b = 1$ *whenever* $k \leqslant 9$. *Then* (2.11) *with* $t = k$, $P(b) < k$ *and* $|R| \geqslant k-1$ *does not hold.*

*Proof.* We assume (2.11) with $t = k, P(b) < k$ and $|R| \geqslant k-1$. Let $k = 6$. By $|R| \geqslant 5$ and (2.27), we derive that at least one $a_i$ is divisible by 5. Further, we see from $b = 1$ that 5 divides $a_0$ and $a_5$. Hence $a_1, a_2, a_3, a_4$ belong to $\{1, 2, 3, 6\}$. If $|R| = k$, then $a_1, a_2, a_3, a_4$ are distinct and this contradicts the result of Euler stated in Section 1. Let $|R| = k-1$. We observe again that $a_1, a_2, a_3, a_4$ are not all distinct. Since $5 \mid a_0$, we have $5 \mid n$. Thus $(a_1/5) = ((n+d)/5) = (d/5)$. Similarly

$$\left(\frac{a_2}{5}\right) = \left(\frac{2d}{5}\right), \qquad \left(\frac{a_3}{5}\right) = \left(\frac{3d}{5}\right), \qquad \left(\frac{a_4}{5}\right) = \left(\frac{4d}{5}\right).$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Hence

$$\left(\frac{a_1}{5}\right) = \left(\frac{a_4}{5}\right) \quad \text{and} \quad \left(\frac{a_2}{5}\right) = \left(\frac{a_3}{5}\right).$$

Thus $a_1, a_4 \in \{1, 6\}, a_2, a_3 \in \{2, 3\}$ or $a_1, a_4 \in \{2, 3\}, a_2, a_3 \in \{1, 6\}$. Therefore we have either $a_1 = a_4 = 1$ or $a_2 = a_3 = 1$. If $a_1 = a_4 = 1$, then $a_2 = 2, a_3 = 3$ or $a_2 = 3, a_3 = 2$. This gives $(a_0, a_1, a_2, a_3, a_4, a_5) = (30, 1, 2, 3, 1, 5)$ or $(5, 1, 3, 2, 1, 30)$. By $a_1 = a_4 = 1$, we see from (2.15) and $d = p^\alpha$ that $d = (2x_1 + 1)/3$ or $2x_1 + 3$. Further from $d^2 = \frac{1}{6}((n + 2d)(n + 3d) - n(n + 5d))$, we get $d^2 = (x_2x_3)^2 - (5x_0x_5)^2$ implying that $d^2 + 1 = 2x_2x_3$. Also $6x_2^2x_3^2 = (x_1^2 + d)(x_1^2 + 2d)$. Hence $24(d^2 + 1)^2 - (d^2 + 2d + 9)(d^2 - 2d + 9) = 0$ if $d = 2x_1 + 3$ and $24(d^2 + 1)^2 - (9d^2 + 2d + 1)(9d^2 - 2d + 1) = 0$ if $d = (2x_1 + 1)/3$. By observing that the constant terms in the above polynomials in $d$ are divisible by $d$, we derive that either $d = 2x_1 + 3 = 3, 19$ or $d = (2x_1 + 1)/3 = 23$. These possibilities are easily excluded. If $a_2 = a_3 = 1$, then $a_1 = 2, a_4 = 3$ or $a_1 = 3, a_4 = 2$. In both cases, we see that $3 \nmid a_0a_5$ and (2.11) with $b = 1$ is not satisfied.

Let $k = 7$. Then, by $b = 1$ and $|R| \geqslant 6$, we may assume that either 5 divides $a_0, a_5$ or 5 divides $a_1, a_6$. Let 5 divide $a_0, a_5$. Then $a_1, a_2, a_3, a_4, a_6 \in \{1, 2, 3, 6\}$ and the repeated element is among $a_1, a_2, a_3, a_4$. Then as in the case $k = 6$, we have either $a_1 = a_4 = 1$ or $a_2 = a_3 = 1$. The first possibility implies that $a_6 = 6, a_3 = 3, a_2 = 2, a_5 = 5, a_0 \in \{10, 15, 30\}$ and we observe that (2.11) with $b = 1$ is not satisfied. In the second possibility, we see that $a_1, a_4, a_6 \in \{2, 3\}$ contradicting $|R| \geqslant 6$. The argument for the case when 5 divides $a_1$ and $a_6$ is similar.

Let $k = 8$. If $|R| = 8$, then we may assume that 7 divides $a_0, a_7$ and 5 divides $a_1, a_6$. Hence $a_2, a_3, a_4, a_5$ is a permutation of $1, 2, 3, 6$ implying $(n + 2d)(n + 3d)(n + 4d)(n + 5d)$ is a square which is impossible by the result of Euler. Let now $|R| = 7$. By $b = 1$, we may assume that 7 divides $a_0, a_7$ and 5 divides $a_0, a_5$ or $a_1, a_6$ or $a_2, a_7$. Let 5 divide $a_1, a_6$. Then $a_2, a_3, a_4, a_5$ belong to $\{1, 2, 3, 6\}$. By mod 7 consideration, we find that either $a_2, a_4$ or $a_3, a_5$ take values from $\{3, 6\}$ which is impossible. Let 5 divide $a_0, a_5$ or $a_2, a_7$. Then by mod 7 and mod 5 considerations, we find that either

$$\begin{aligned} &n = 35x_0^2, n + d = x_1^2, n + 2d = 2x_2^2, n + 3d = 3x_3^2, n + 4d = x_4^2, n + 5d = 5x_5^2, \\ &\quad n + 6d = 6x_6^2, n + 7d = 7x_7^2 \end{aligned}$$

or

$$\begin{aligned} &n = 7x_0^2, n + d = 6x_1^2, n + 2d = 5x_2^2, n + 3d = x_3^2, n + 4d = 3x_4^2, n + 5d = 2x_5^2, \\ &\quad n + 6d = x_6^2, n + 7d = 35x_7^2. \end{aligned}$$

We give the argument for the first possibility. We have $x_4^2 - x_1^2 = 3d$. Hence $x_4 - x_1 = 1$ or 3 giving

$$d = p^\alpha = \frac{2x_1 + 1}{3} \quad \text{or} \quad 2x_1 + 3. \tag{6.1}$$

Also we note that $\gcd(x_1, 210) = 1$ implying $x_1 \geqslant 11$. Further

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{n}{p}\right) = 1$$

which, together with (6.1), implies that $d \geqslant 163$. We observe that $(n+2d)(n+3d)(n+6d) = (6x_2x_3x_6)^2$ which gives

$$9x_1^6 + 48x_1^5 + 92x_1^4 + \frac{284}{3}x_1^3 + 57x_1^2 + 20x_1 + \frac{10}{3} = Y_1^2$$

with $Y_1 = 18x_2x_3x_6$ if $d = (2x_1+1)/3$ and

$$x_1^6 + 16x_1^5 + 92x_1^4 + 284x_1^3 + 513x_1^2 + 540x_1 + 270 = Y_2^2$$

with $Y_2 = 6x_2x_3x_6$ if $d = 2x_1 + 3$. In the former case we take square root on both sides to get

$$9x_1^3 + 24x_1^2 + 14x_1 + 9 < 3Y_1 < 9x_1^3 + 24x_1^2 + 14x_1 + 10$$

which is impossible. In the latter case we observe from $d \geqslant 163$ that $x_1 \geqslant 80$ and then we take square root on both the sides to obtain

$$x_1^3 + 8x_1^2 + 14x_1 + 29 < Y_2 < x_1^3 + 8x_1^2 + 14x_1 + 30,$$

a contradiction. The second possibility is excluded similarly.

Let $k = 9$. Then we may assume that 7 divides two $a_i$'s and 5 divides two other $a_i$'s. Thus we have 7 divides $a_0, a_7$, 5 divides $a_1, a_6$ or 5 divides $a_3, a_8$; 7 divides $a_1, a_8$, 5 divides $a_0, a_5$ or 5 divides $a_2, a_7$. We take the possibility 7 dividing $a_0, a_7$, 5 dividing $a_1, a_6$. By using Legendre Symbol mod 7, we see that $a_2, a_4, a_8 \in \{1, 2\}$, $a_3, a_5 \in \{3, 6\}$ or $a_2, a_4, a_8 \in \{3, 6\}$, $a_3, a_5 \in \{1, 2\}$. Since $a_3$ and $a_5$ are not both divisible by 3 and $a_2, a_4, a_8$ are all not divisible by 3, this is excluded. The argument for other possibilities is similar.

When $k = 10, 11$, we get $f(2) \geqslant 5$ contradicting (2.27). □

LEMMA 8. *Assume* (2.11) *with* $P(b) < k$. *Let* $k \geqslant 12$ *such that* $k-1$ *is prime and* $d \neq 2, 4$.

(a) *If* $d = p^\alpha$ *and* $t = k-1$, *let* $k \geqslant 30$. *Then* $|R| \leqslant t - M - 1$ *where* $M$ *is given by* (2.21).
(b) *Let* $k \geqslant 68$ *if* $d = p^\alpha$; $k \geqslant 54$ *if* $d = 12p^\alpha$; $k \geqslant 30$ *if* $d = 3p^\alpha, 3 \cdot 2^\alpha, 5 \cdot 2^\alpha, 7 \cdot 2^\alpha, 9 \cdot 2^\alpha$; $k \geqslant 18$ *if* $d = 2^\alpha$ *and* $k \geqslant 38$ *otherwise. Then* $|R| \leqslant t - 4M - 1$.

The assumption $k-1$ prime is not used when $k > 210$ if $d = p^\alpha$ and $k > 160$ if $d \neq p^\alpha$.

*Proof*. We assume (2.11) with $P(b) < k$. We recall that $a_i$'s are square free and $P(a_i) < k$. We shall denote by $p_0$ any prime $< k$. We put $\gamma_{p_0} = \mathrm{ord}_{p_0}\left(\prod_{a_i \in R} a_i\right)$. It is clear that

$$\gamma_{p_0} \leqslant \left[\frac{k-1}{p_0}\right] + 1. \tag{6.2}$$

Since

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

$$\prod_{a_i \in R} a_i = \prod_{p_0 < k} p_0^{\gamma_{p_0}},$$

it follows that

$$\prod_{a_i \in R} a_i \,\Big|\, (k-1)! \prod_{p_0 < k} p_0. \tag{6.3}$$

Let

$$\gamma'_{p_0} = \mathrm{ord}_{p_0}\left((k-1)! \prod_{p_0 < k} p_0\right).$$

Suppose $p_0^h \leqslant k-1 < p_0^{h+1}$ where $h$ is a positive integer. Then

$$\gamma'_{p_0} = \left[\frac{k-1}{p_0}\right] + \left[\frac{k-1}{p_0^2}\right] + \cdots + \left[\frac{k-1}{p_0^h}\right] + 1.$$

The estimate for $\gamma_{p_0}$ given in (6.2) can be improved as follows. We observe that $\gamma_{p_0} = 0$ if $p_0 \mid d$. Let $p_0 \nmid d$. Then we see that $\gamma_{p_0}$ equals the number of terms in $\{n + d_1 d, \ldots, n + d_t d\}$ divisible by $p_0$ to an odd power. We remove from the above set a term in which $p_0$ appears to a maximum power. The number of terms in the remaining set divisible by $p_0$ to an odd power is at most

$$\left[\frac{k-1}{p_0}\right] - \left(\left[\frac{k-1}{p_0^2}\right] - 2\right) + \left[\frac{k-1}{p_0^3}\right] - \left(\left[\frac{k-1}{p_0^4}\right] - 2\right) + \cdots + (-1)^{\epsilon_3} \times$$
$$\times \left(\left[\frac{k-1}{p_0^h}\right] - 1 + (-1)^{\epsilon_3}\right),$$

where $\epsilon_3 = 1$ or 0 according as $h$ is even or odd, respectively. Note that the above expression is always positive. Thus we obtain

$$\begin{aligned}
\gamma_{p_0} - \gamma'_{p_0} &\leqslant h - 1 + \epsilon_3 - 2\left(\left[\frac{k-1}{p_0^2}\right] + \cdots + \left[\frac{k-1}{p_0^{h-1+\epsilon_3}}\right]\right) \\
&\leqslant h - 1 + \epsilon_3 - 2\left(\frac{k-1}{p_0^2} + \cdots + \frac{k-1}{p_0^{h-1+\epsilon_3}} - \frac{h-1+\epsilon_3}{2}\right) \\
&= 2h - 2 + 2\epsilon_3 - \frac{2(k-1)}{p_0^2 - 1}\left(1 - \frac{1}{p_0^{h-1+\epsilon_3}}\right).
\end{aligned}$$

Since $p_0^h > (k-1)/p_0$ and $h < \log k / \log p_0$, we get

$$\gamma_{p_0} - \gamma'_{p_0} < -\frac{2k}{p_0^2 - 1} + \frac{2 \log k}{\log p_0} + \frac{2 + 2p_0^{2-\epsilon_3}}{p_0^2 - 1} + 2\epsilon_3 - 2.$$

Thus we see that

$$\gamma_{p_0} - \gamma'_{p_0} < -\frac{2k}{p_0^2 - 1} + \frac{2 \log k}{\log p_0} + \epsilon_4 \tag{6.4}$$

where

$$\epsilon_4 = \begin{cases} 2, & \text{if } p_0 = 2, \\ 1, & \text{if } p_0 = 3, \\ \frac{1}{2}, & \text{if } p_0 = 5, \\ \frac{1}{3}, & \text{if } p_0 = 7. \end{cases} \tag{6.5}$$

From (6.3) we get

$$\prod_{a_i \in R} a_i \,\Big|\, (k-1)! \prod_{p_0 < k} p_0 \prod_{p_0 \leqslant 7} p_0^{\gamma_{p_0} - \gamma'_{p_0}}. \tag{6.6}$$

Using (6.4) and (6.5) we estimate $\prod_{p_0 \leqslant 7} p_0^{\gamma_{p_0} - \gamma'_{p_0}} \leqslant 52\, k^8 (2.5907)^{-k}$. From [9, p. 71] we get $\prod_{p_0 < k} p_0 \leqslant (2.78)^k$. Thus (6.6) implies that

$$\prod_{a_i \in R} a_i \leqslant 52(k-1)! k^8 (1.0731)^k. \tag{6.7}$$

Let $d = p^\alpha$. Then $M = 1$ by (2.21). Assume that $|R| \geqslant k - 5$ which is satisfied if $|R| > t - 4M - 1$ since $t \geqslant k - 1$. Then

$$\prod_{a_i \in R} a_i \geqslant \prod_{i=1}^{k-5} s_i \tag{6.8}$$

where $s_i$ denotes the $i$th square free integer. We first show that

$$s_i \geqslant 1.5\, i \quad \text{for } i \geqslant 39. \tag{6.9}$$

We check that (6.9) is valid for $39 \leqslant i \leqslant 70$. Let $i \geqslant 71$. We write $s_i = 36\mu + \nu$, where $\mu$ and $\nu$ are integers with $\mu > 0$, $0 \leqslant \nu < 36$ and $\nu \notin \{0, 4, 8, 9, 12, 16, 18, 20, 24, 27, 28, 32\}$. Further we check that for any integer $\nu$ as above, we can choose an integer $i_\nu$ such that $39 \leqslant i_\nu \leqslant 70$, $s_{i_\nu} \equiv \nu (\mathrm{mod}\ 36)$. Then $s_i - s_{i_\nu} = 36\eta$ for some integer $\eta > 0$. By deleting multiples of 4 and 9, we find that in any set of 36 consecutive integers, the number of square free integers is $\leqslant 24$. Thus the number of square free integers in $(s_{i_\nu}, s_i]$ is at most $24\eta$. Therefore $i - i_\nu \leqslant \frac{2}{3}(s_i - s_{i_\nu})$. Hence $s_i \geqslant 1.5(i - i_\nu) + s_{i_\nu} \geqslant 1.5\, i$ since $s_{i_\nu} \geqslant 1.5\, i_\nu$ for $39 \leqslant i_\nu \leqslant 70$. This proves (6.9). Now we use (6.9) to get $\prod_{i=1}^{k-5} s_i \geqslant (1.5)^{k-5}(k-5)!$ for $k \geqslant 68$, by induction on $k$. Thus by (6.8), we have

$$\prod_{a_i \in R} a_i \geqslant (1.5)^{k-5}(k-5)! \quad \text{for } k \geqslant 68. \tag{6.10}$$

We combine (6.7) and (6.10) to get $(1.3978)^k \leqslant 395\, k^{12}$ for $k \geqslant 68$ which implies that $k \leqslant 210$. Now we check that $f_0(4) \geqslant 17$ for $68 \leqslant k \leqslant 139$; $f_0(5) \geqslant 33$ for $140 \leqslant k \leqslant 210$. This is a contradiction by (2.26) and (2.27). Thus $k \leqslant 67$ if $|R| \geqslant k - 5$. Further we check that $f_0(3) \geqslant 9$ for $30 \leqslant k \leqslant 67$ if $|R| \geqslant k - 2$. Thus it remains to consider only the cases $k = 12, 14, 18, 20, 24$ with $t = k$ and $|R| \geqslant k - 1$. Then we have $f_0(3) \geqslant 8$ for $k = 24$ and $f_0(2) \geqslant 4$ for $k \in \{12, 14, 18, 20\}$. By (2.27), we derive that $f_0(3) = 8$ for $k = 24$ and $f_0(2) = 4$ for

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

$k \in \{12, 14, 18, 20\}$. Let $k = 24$. Since $f_0(3) = 8$, we see that $|R| = k - 1$. Further the number of $i$'s for which $a_i$'s are divisible by the primes $23, 19, 17, 13, 11, 7$ is exactly $2, 2, 2, 2, 3, 4$, respectively, and none of these $a_i$'s is divisible by more than one of these primes. Hence 23 divides $a_0, a_{23}$ ; 7 divides $a_1, a_8, a_{15}, a_{22}$. Then 11 does not divide three other $a_i$'s. This is a contradiction. Thus $k \neq 24$. The other cases are excluded similarly. This completes the proof of Lemma 8 when $d = p^\alpha$.

Now we take $d \neq p^\alpha$. Let $k$ be as in Lemma 8(b) and assume that $|R| > t - 4M - 1$ which implies that $|R| \geqslant k - 4M - 1$. Let $d = 2p^\alpha$. Then $M = 2$ by (2.21) and $|R| \geqslant k - 9$. Hence by (2.20), we have

$$\prod_{a_i \in R} a_i \geqslant \prod_{i=1}^{k-9} (2i - 1) \geqslant \prod_{i=2}^{k-9} 2(i - 1) = 2^{k-10}(k - 10)!$$

Similarly, we find that $\prod_{a_i \in R} a_i$ exceeds

$8^{k-10}(k - 10)!$ if $d = 2^\alpha$; $3^{k-10}(k - 10)!$ if $d = 3p^\alpha$; $4^{k-14}(k - 14)!$ if $d = 4p^\alpha$;
$(2.5)^{k-11}(k - 11)!$ if $d = 5p^\alpha$; $6^{k-18}(k - 18)!$ if $d = 6p^\alpha$; $(\frac{7}{3})^{k-11}(k - 11)!$ if $d = 7p^\alpha$;
$8^{k-18}(k - 18)!$ if $d = 8p^\alpha$; $3^{k-10}(k - 10)!$ if $d = 9p^\alpha$; $5^{k-19}(k - 19)!$ if $d = 10p^\alpha$;
$12^{k-26}(k - 26)!$ if $d = 12p^\alpha$; $24^{k-18}(k - 18)!$ if $d = 3 \cdot 2^\alpha$ with $\alpha \geqslant 3$;
$12^{k-18}(k - 18)!$ if $d = 12$; $20^{k-19}(k - 19)!$ if $d = 5 \cdot 2^\alpha$;
$(\frac{56}{3})^{k-21}(k - 21)!$ if $d = 7 \cdot 2^\alpha$; $24^{k-18}(k - 18)!$ if $d = 9 \cdot 2^\alpha$.

Now we combine these lower bounds with the upper bound (6.7) to conclude that $k \leqslant 160$. To bring down the value of $k$ we use the counting argument as in the case $d = p^\alpha$. We obtain $k \leqslant 98$ if $d = 8p^\alpha, 12p^\alpha$; $k \leqslant 62$ if $d = 4p^\alpha$; $k \leqslant 54$ if $d = 6p^\alpha$, $3 \cdot 2^\alpha, 5 \cdot 2^\alpha, 7 \cdot 2^\alpha, 9 \cdot 2^\alpha$ and $k \leqslant 32$ otherwise. Finally, we use a congruence argument to complete the proof of Lemma 8(b). We explain one instance. Let $d = 8p^\alpha$. By counting argument we get $k \leqslant 98$. Now we use the fact that $a_i \equiv a_j \pmod 8$ for all $i, j$ with $0 \leqslant i, j \leqslant t$ to find that $k \leqslant 32$.

For Lemma 8(a), we assume that $|R| > t - M - 1 \geqslant k - M - 2$. Then it remains to consider only those values of $k$ not covered in Lemma 8(b). We use counting argument to exclude all values of $k$ other than $k = 12, 14, d = 4p^\alpha$; $k = 12, 14, 18, 20, 24, d = 8p^\alpha$; $k = 12, 14, d = 12p^\alpha$ and $k = 12, 14, d = 7p^\alpha$. All the cases other than the last one are excluded by congruence argument given above. Let now $k = 12, 14$ and $d = 7p^\alpha$. Then $7 \nmid a_i$ for any $i$ and $f_0(2) = 4$. If $k = 12$, this implies that 11 divides $a_0, a_{11}$ and 5 divides 3 other $a_i$'s which is impossible. If $k = 14$, we find that 13 divides $a_0, a_{13}$, 11 divides $a_1, a_{12}$ and 5 divides 3 other $a_i$'s which is again impossible. □

LEMMA 8′. *If* $d = 2, 4$, *then* (2.11) *with either* $P(b) \leqslant k$ *if* $t = k$ *or* $P(b) < k$ *if* $t = k - 1$ *does not hold.*

*Proof.* Let $d = 2, 4$. Suppose $|R| < t$. Then there exists $i, j$ with $0 \leqslant j < i \leqslant t$ such that $a_i = a_j = a$, say, and (3.1) holds. As $d$ is even, we have $x_i, x_j$ odd. Thus

$x_i \geqslant x_j + 2$. Further, by (2.13), we get $n \geqslant k^2 - 2k + 5 > (k-1)^2$. Therefore

$$4(k-1) \geqslant (i-j)d = a(x_i^2 - x_j^2) \geqslant 4ax_j \geqslant 4(ax_j^2)^{\frac{1}{2}} \geqslant 4n^{\frac{1}{2}} > 4(k-1),$$

a contradiction. Hence $|R| = t$. As in Lemma 8, we see that (6.7) holds and $\prod_{a_i \in R} a_i$ exceeds $2^{k-2}(k-2)!$ implying $k \leqslant 75$. Now we use counting argument to conclude that $k \leqslant 11$ and the assertion follows from Lemma 2. □

In view of Lemma 8′, we suppose that $d \neq 2, 4$ from now on throughout the paper. Thus $\alpha \geqslant 3$ whenever $d = 2^\alpha$.

## 7. Upper Bound for $n + (k-1)d$

We suppose that (2.11) with $P(b) < k$ is satisfied. Further we suppose that $k \geqslant 6$ if $d = p^\alpha, t = k$; $k \geqslant 30$ if $d = p^\alpha, t = k-1$ and $k \geqslant 12$ otherwise. Also let $b = 1$ whenever $k \leqslant 9$. We bound $n$ from above by $C_4k^3$ and $d$ by $C_5k$ where $C_4$ and $C_5$ are constants depending on $\chi$. We find that the constants $C_4$ and $C_5$ are small since $\chi \leqslant 12$. Thus we get rather good upper bounds for $n$ and $d$. To achieve this, we proceed as follows. Lemmas 2,7 and 8 guarantee that $|R| \leqslant t - M - 1$ under some restrictions on $k$. This bound on $|R|$ gives rise to two cases. In the first case, there is an $a_i$ being repeated more than two times. This case is treated in Lemma 9. In the second case, there exist distinct integers $\mu_0, \mu_1, \nu_0, \nu_1$ with $a_{\mu_0} \neq a_{\nu_0}, a_{\mu_0} = a_{\mu_1}, a_{\nu_0} = a_{\nu_1}$ and there exists a partititon of $d$ corresponding to both $a_{\mu_0} = a_{\mu_1}, a_{\nu_0} = a_{\nu_1}$. This case is treated in Lemmas 10 and 11. Here we use an argument of Shorey and Tijdeman [16, Lemma 2]. For large values of $k$, we have $|R| \leqslant t - 4M - 1$ by Lemma 8(b) and refining the above procedure we obtain sharper estimates for $n$ and $d$, see Lemma 11. The proofs of the Lemmas 9 and 10 can be adapted for any $d$ whereas the proof of Lemma 11 can be adapted for any $d$ with $\omega(d)$ bounded.

LEMMA 9. *Suppose that one of the following possibilities hold.*

(a) $R_1^{(i)} \neq \phi$ *for some* $i \geqslant 3$.
(b) *Let* $a_i = a_j$ *with* $i > j$ *and* $\frac{d}{\chi_1} \nmid h_2$ *for some partition* $(h_1, h_2)$ *of* $d$ *corresponding to* $a_i = a_j$.

*Then*

$$n < \frac{(k-1)^2\chi_1^2}{4\epsilon_0^2}, \qquad d < \frac{(k-1)\chi_1^2}{\epsilon_0^2}. \tag{7.1}$$

*Proof.* Suppose (a) holds. Let $\mu_0 \in R_1^{(i)}$ with $i \geqslant 3$. Then there exist integers $\mu_1, \mu_2$ with $\mu_0 > \mu_1 > \mu_2$ such that

$$(\mu - \nu)d = a_\nu(x_\mu - x_\nu)(x_\mu + x_\nu) \tag{7.2}$$

is valid for $(\mu, \nu)$ satisfying (4.9). Also there exists $(\mu, \nu)$ from (4.9) and a partition $(h_1, h_2)$ of $d$ corresponding to $a_\mu = a_\nu$ such that $d/\chi_1 \mid h_1$. Thus $d/\chi_1 \mid (x_\mu - x_\nu)$.

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Further if $d$ is even and $d/\chi_1$ is odd, we find that $2d/\chi_1 \mid (x_\mu - x_\nu)$ since $x_\mu - x_\nu$ is even. Then we see from (7.2) and (2.23) that

$$k - 1 \geqslant \mu - \nu > \frac{2\epsilon_0}{\chi_1}(a_\nu x_\nu^2)^{\frac{1}{2}} \geqslant \frac{2\epsilon_0}{\chi_1} n^{\frac{1}{2}} \tag{7.3}$$

and

$$k - 1 \geqslant \mu - \nu \geqslant \frac{a_\nu \epsilon_0}{\chi_1}\left(2x_\nu + \frac{d\epsilon_0}{\chi_1}\right) > \frac{d\epsilon_0^2}{\chi_1^2}. \tag{7.4}$$

Now we derive (7.1) from (7.3) and (7.4).

Suppose (b) holds. Then (7.2) is valid with $(\mu, \nu) = (i, j)$. Since for the partition $(h_1, h_2)$ of $d$ corresponding to $a_i = a_j$ we have $d/\chi_1 \nmid h_2$, we find that $d/\chi_1 \mid h_1$. Now we argue as in the preceding paragraph to obtain (7.3), (7.4) which imply (7.1). □

LEMMA 10. *Let* $\mu_0, \nu_0 \in R_1^{(2)}$ *with* $\mu_0 \neq \nu_0$ *and*

$$a_{\mu_0} = a_{\mu_1}, \quad a_{\nu_0} = a_{\nu_1}. \tag{7.5}$$

*Suppose that there exists a partition* $(h_1, h_2)$ *of* $d$ *corresponding to both* $a_{\mu_0} = a_{\mu_1}$ and $a_{\nu_0} = a_{\nu_1}$ *with* $d/\chi_1 \mid h_2$. *Let* $c > 0$. *If*

$$|\mu_0 - \nu_0| \leqslant \frac{k-1}{c}, \quad |\mu_1 - \nu_1| \leqslant \frac{k-1}{c}, \tag{7.6}$$

*then*

$$d < 2\epsilon_1\chi_1(k-1)\left(1 + \frac{1}{c}\right) \tag{7.7}$$

*and*

$$n < (k-1)^2 \min\left(\frac{\epsilon_2 d}{4}, \frac{\epsilon_2^2(k-1)}{c} + \frac{\epsilon_1\chi_1}{4}\right). \tag{7.8}$$

*Proof.* Since $\mu_0 > \mu_1$ and $\nu_0 > \nu_1$, we see that $x_{\mu_0} > x_{\mu_1}$ and $x_{\nu_0} > x_{\nu_1}$. Let $(h_1, h_2)$ be a partition of $d$ corresponding to both $a_{\mu_0} = a_{\mu_1}$ and $a_{\nu_0} = a_{\nu_1}$. We put $\epsilon' = \gcd(h_1, h_2)$ and we observe that $\epsilon' \leqslant \epsilon_2$ where $\epsilon_2$ is given by (2.25). We write

$$x_{\mu_0} - x_{\mu_1} = h_1 r_1, \qquad x_{\mu_0} + x_{\mu_1} = h_2 r_2; \qquad x_{\nu_0} - x_{\nu_1} = h_1 s_1, \qquad x_{\nu_0} + x_{\nu_1} = h_2 s_2,$$

where $r_1, r_2, s_1, s_2$ are some positive integers. Further, we see from (2.15) that

$$\begin{aligned}(\mu_0 - \nu_0)d = a_{\mu_0}x_{\mu_0}^2 - a_{\nu_0}x_{\nu_0}^2 &= a_{\mu_0}\left(\frac{h_2 r_2 + h_1 r_1}{2}\right)^2 - a_{\nu_0}\left(\frac{h_2 s_2 + h_1 s_1}{2}\right)^2 \\ &= \tfrac{1}{4}\{(a_{\mu_0} r_1^2 - a_{\nu_0} s_1^2)h_1^2 + (a_{\mu_0} r_2^2 - a_{\nu_0} s_2^2)h_2^2 + 2(a_{\mu_0} r_1 r_2 - a_{\nu_0} s_1 s_2)h_1 h_2\}.\end{aligned}$$

Hence, we see that

$$\frac{h_1}{\epsilon'} \,\Big|\, (a_{\mu_0} r_2^2 - a_{\nu_0} s_2^2); \qquad \frac{h_2}{\epsilon'} \,\Big|\, (a_{\mu_0} r_1^2 - a_{\nu_0} s_1^2).$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

Thus there exist non-zero integers $f_1, f_2$ such that

$$\frac{f_1 h_1 h_2^2}{\epsilon'} = a_{\mu_0}(x_{\mu_0} + x_{\mu_1})^2 - a_{\nu_0}(x_{\nu_0} + x_{\nu_1})^2$$

and

$$\frac{f_2 h_1^2 h_2}{\epsilon'} = a_{\mu_0}(x_{\mu_0} - x_{\mu_1})^2 - a_{\nu_0}(x_{\nu_0} - x_{\nu_1})^2. \tag{7.9}$$

Therefore, from (7.5) we have

$$\frac{f_1 h_1 h_2^2}{\epsilon'} = (a_{\mu_0}x_{\mu_0}^2 - a_{\nu_0}x_{\nu_0}^2) + (a_{\mu_1}x_{\mu_1}^2 - a_{\nu_1}x_{\nu_1}^2) + 2(a_{\mu_0}x_{\mu_0}x_{\mu_1} - a_{\nu_0}x_{\nu_0}x_{\nu_1}) \tag{7.10}$$

and

$$\frac{f_2 h_1^2 h_2}{\epsilon'} = (a_{\mu_0}x_{\mu_0}^2 - a_{\nu_0}x_{\nu_0}^2) + (a_{\mu_1}x_{\mu_1}^2 - a_{\nu_1}x_{\nu_1}^2) - 2(a_{\mu_0}x_{\mu_0}x_{\mu_1} - a_{\nu_0}x_{\nu_0}x_{\nu_1}). \tag{7.11}$$

Further, from

$$\begin{aligned}(\mu_1 - \nu_0)d = a_{\mu_1}x_{\mu_1}^2 - a_{\nu_0}x_{\nu_0}^2 &< a_{\mu_0}x_{\mu_0}x_{\mu_1} - a_{\nu_0}x_{\nu_0}x_{\nu_1} < a_{\mu_0}x_{\mu_0}^2 - a_{\nu_1}x_{\nu_1}^2 \\ &= (\mu_0 - \nu_1)d\end{aligned}$$

we get

$$|a_{\mu_0}x_{\mu_0}x_{\mu_1} - a_{\nu_0}x_{\nu_0}x_{\nu_1}| < (k-1)d. \tag{7.12}$$

We see from (7.10), (7.12) and (7.6) that

$$h_2 < 2\epsilon'(k-1)\left(1 + \frac{1}{c}\right). \tag{7.13}$$

Further since $d/\chi_1 \mid h_2$, we get from (2.2) that

$$h_1 \leqslant \begin{cases} \chi_1, & \text{always,} \\ \frac{\chi_1}{2}, & \text{if } \gcd(h_1, h_2) = 2, d \neq \chi 2^{\alpha}, \end{cases} \tag{7.14}$$

which, together with (7.13) and (2.24), gives (7.7). We obtain from (7.11) and (7.6) that

$$2|a_{\mu_0}x_{\mu_0}x_{\mu_1} - a_{\nu_0}x_{\nu_0}x_{\nu_1}| \leqslant \frac{2(k-1)d}{c} + \frac{|f_2|h_1 d}{\epsilon'}.$$

We use this inequality in (7.10) to get

$$h_2 \leqslant \frac{\epsilon'}{|f_1|}\left(\frac{4(k-1)}{c} + \frac{|f_2|h_1}{\epsilon'}\right). \tag{7.15}$$

Also from (7.9) we get

$$\frac{|f_2|h_1^2 h_2}{\epsilon'} \leqslant \max(a_{\mu_0}(x_{\mu_0} - x_{\mu_1})^2, a_{\nu_0}(x_{\nu_0} - x_{\nu_1})^2). \tag{7.16}$$

We know from (2.15) and $x_{\mu_0} > x_{\mu_1}, x_{\nu_0} > x_{\nu_1}$ that

$$n < \tfrac{1}{4}a_{\mu_0}(x_{\mu_0} + x_{\mu_1})^2, \qquad n < \tfrac{1}{4}a_{\nu_0}(x_{\nu_0} + x_{\nu_1})^2. \tag{7.17}$$

We combine (7.16) and (7.17) to get

$$\frac{|f_2|h_1^2 h_2 n}{\epsilon'} < \max(\tfrac{1}{4}(a_{\mu_0}x_{\mu_0}^2 - a_{\mu_1}x_{\mu_1}^2)^2, \tfrac{1}{4}(a_{\nu_0}x_{\nu_0}^2 - a_{\nu_1}x_{\nu_1}^2)^2).$$

Hence, we have $n < \epsilon'/(4|f_2|)(k-1)^2 h_2$ which, by $h_2 \leqslant d$, (7.15), (7.14) and (2.24), implies (7.8). $\square$

Using Lemma 10 we derive the following lemma.

LEMMA 11. *Let* $k-1$ *be prime if* $k \geqslant 12$. *Suppose* (a) *and* (b) *of Lemma* 9 *do not hold. Then the following are valid.*

(i) *We have*

$$n < (k-1)^2 \min\left(\frac{\epsilon_2 d}{4}, \epsilon_2^2(k-1) + \frac{\epsilon_1\chi_1}{4}\right), \qquad d < 4\epsilon_1\chi_1(k-1).$$

(ii) *For* $k$ *satisfying the assumptions of Lemma* 8(b), *we have*

$$n < (k-1)^2 \min\left(\frac{\epsilon_2 d}{4}, \frac{\epsilon_2^2(k-1)}{2} + \frac{\epsilon_1\chi_1}{4}\right), \qquad d < 3\epsilon_1\chi_1(k-1).$$

*Proof.* Since (a) and (b) of Lemma 9 do not hold, we have $R_1^{(i)} = \phi$ for $i \geqslant 3$ and if $a_i = a_j$ with $i > j$ then for every possible partition $(h_1, h_2)$ of $d$ corresponding to $a_i = a_j$, we have $d/\chi_1 \mid h_2$.

(i) By Lemma 8(a), we derive that $|R| \leqslant t - M - 1$ for $k \geqslant 12$. This is also the case for $d = p^\alpha$ with $k \leqslant 11$ by Lemma 7 and $M = 1$. Then there exists at least $M+1$ distinct pairs $(\mu, \nu)$ with $\mu > \nu$, $\mu \in R_1^{(2)}$, $a_\mu = a_\nu$ and (7.2) holds. Further since $d/\chi_1 \mid h_2$, the number of partitions $(h_1, h_2)$ of $d$ corresponding to $a_\mu = a_\nu$ equals $M$. Therefore there exist distinct $\mu_0, \nu_0 \in R_1^{(2)}$ and $\mu_1, \nu_1$ with $\mu_0 > \mu_1$, $\nu_0 > \nu_1$ satisfying (7.5) and a partition $(h_1, h_2)$ of $d$ corresponding to both $a_{\mu_0} = a_{\mu_1}$ and $a_{\nu_0} = a_{\nu_1}$. Further (7.6) holds with $c = 1$. Hence, by Lemma 10, we conclude that (7.7) and (7.8) with $c = 1$ hold implying the assertion.

(ii) By Lemma 8(b), we derive that $|R| \leqslant t - 4M - 1$. We argue as in (i) to find that there is a partition $(h_1, h_2)$ corresponding to the five relations

$$a_{\mu_0} = a_{\mu_1}, \qquad a_{\nu_0} = a_{\nu_1}, \qquad a_{\tau_0} = a_{\tau_1}, \qquad a_{\psi_0} = a_{\psi_1}, \qquad a_{\zeta_0} = a_{\zeta_1}$$

where $\mu_0, \nu_0, \tau_0, \psi_0, \zeta_0$ are distinct elements of $R_1^{(2)}$. Further we see that there exist two pairs, say, $(\mu_0, \mu_1)$ with $\mu_0 > \mu_1$ and $(\nu_0, \nu_1)$ with $\nu_0 > \nu_1$ such that

$$|\mu_0 - \nu_0| \leqslant \frac{k-1}{2}, |\mu_1 - \nu_1| \leqslant \frac{k-1}{2}.$$

Thus (7.6) is satisfied with $c = 2$. Hence, by Lemma 10, we derive that (7.7) and (7.8) with $c = 2$ are valid. Now the assertion follows immediately. $\square$

## 8. $n, d, k$ are Bounded

We assume (2.11) with $P(b) < k$. Further we suppose that $k$ satisfies the assumptions stated in the begining of Section 7 and $k-1$ is prime if $k \geqslant 12$. We combine Lemmas 9 and 11 to derive an upper bound for $d$ and $n+(k-1)d$ in terms of $k$. Further using the lower estimate for $n+(k-1)d$ from Corollary 3, we show that $k$ is bounded by an absolute constant. Therefore $n$ and $d$ are also bounded by an absolute constant.

LEMMA 12. (i) *Let* $d \neq \chi\tau^{\alpha}$ *with* $\chi \in \{5, 7, 9\}$. *Then*

$$d < 4\epsilon_1\chi_1(k-1). \tag{8.1}$$

*If* $k$ *satisfies the assumptions of Lemma* 8(b), *then*

$$d < 3\epsilon_1\chi_1(k-1). \tag{8.2}$$

(ii) *Let* $d = \chi\tau^{\alpha}$ *with* $\chi \in \{5, 7, 9\}$. *Then*

$$d < (k-1)\frac{\chi_1^2}{\epsilon_0^2}. \tag{8.3}$$

(iii) *Let* $d \neq \{12, 40, 56, 144\}$. *If* $d < 4\epsilon_1\chi_1(k-1)$, *then*

$$n+(k-1)d < \min\left((k-1)^2\frac{\epsilon_2 d}{4} + (k-1)d,\ k^3\left(\epsilon_2^2 + \frac{17\epsilon_1\chi_1}{4k}\right)\right). \tag{8.4}$$

*If* $k$ *satisfies the assumptions of Lemma* 8(b) *and* $d < 3\epsilon_1\chi_1(k-1)$, *then*

$$n+(k-1)d < \min\left((k-1)^2\frac{\epsilon_2 d}{4} + (k-1)d, k^3\left(\frac{\epsilon_2^2}{2} + \frac{13\epsilon_1\chi_1}{4k}\right)\right). \tag{8.5}$$

(iv) *Let* $d = \chi\tau^{\alpha}$ *with* $\chi \in \{5, 7, 9\}$. *Suppose that* $d \geqslant 3\epsilon_1\chi_1(k-1)$ *if* $k$ *satisfies the assumptions of Lemma* 8(b) *and* $d \geqslant 4\epsilon_1\chi_1(k-1)$ *otherwise. Then*

$$n+(k-1)d < \min\left(\frac{(k-1)^2\chi_1^2}{4\epsilon_0^2} + (k-1)d, \frac{5k^2\chi_1^2}{4\epsilon_0^2}\right). \tag{8.6}$$

(v) *Let* $d \in \{12, 40, 56, 144\}$. *Then* (8.6) *holds.*

*Proof.* First we consider the case that (a) and (b) of Lemma 9 do not hold. Then the assertions of Lemma 11 are valid. Thus, we need not consider (iv). Further, (i) and (iii) follow directly from Lemma 11. In fact (8.4) is also valid for $d = 12, 40, 56, 144$. Further, we observe that (8.4) with $d = 12, 40, 56, 144$ implies (8.6). Thus it remains to prove (ii). Let $d = \chi\tau^{\alpha}$ with $\chi \in \{5, 7, 9\}$. Then $d < 4\epsilon_1\chi_1(k-1)$ by Lemma 11(i). Further, we observe that $4\epsilon_1\chi_1 < \chi_1^2/\epsilon_0^2$. Hence, $d < (k-1)\chi_1^2/\epsilon_0^2$. This proves (ii).

Next we suppose that (a) or (b) of Lemma 9 holds. Then (7.1) is valid. Further, we observe that (7.1) implies (8.6). This proves (iv) and (v). Let $d \neq 12, 40, 56, 144$. We see that (7.1) with $d < 4\epsilon_1\chi_1(k-1)$ implies (8.4). Further (7.1) with $d < 3\epsilon_1\chi_1(k-1)$ implies (8.5) whenever $k$ satisfies the assumptions of Lemma 8(b). This proves (iii). Also we see that (ii) is immediate from (7.1). Finally (8.2) follows from the estimate for $d$ in (7.1) whenever $d \neq \chi\tau^{\alpha}$ with $\tau \in \{5, 7, 9\}$. This proves (i). □

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

As a consequence of Lemma 12 and Corollary 3 we get

LEMMA 13. *We have* $k \leqslant \kappa = \kappa(d)$ *where* $(\kappa, d)$ *is given by*

$$\begin{aligned}&(102, p^{\alpha}), (44, 2p^{\alpha}), (24, 3p^{\alpha}), (74, 4p^{\alpha}), (54, 5p^{\alpha}), (38, 6p^{\alpha}),\\ &(74, 7p^{\alpha}), (84, 8p^{\alpha}), (74, 9p^{\alpha}), (48, 10p^{\alpha}), (54, 12p^{\alpha}), (32, 2^{\alpha}),\\ &(54, 3\cdot 2^{\alpha}), (62, 5\cdot 2^{\alpha}), (98, 7\cdot 2^{\alpha}), (84, 9\cdot 2^{\alpha}).\end{aligned} \tag{8.7}$$

*Proof.* Let $d = p^{\alpha}$. Then $\chi_1 = \epsilon_1 = \epsilon_2 = 1$. By Lemma 12(i), we see that $d < 3(k-1)$ for $k \geqslant 68$. Then (8.5) with $k \geqslant 68$ is valid by Lemma 12(iii). Thus $\delta \leqslant \frac{1}{2} + 13/4k$ if $k \geqslant 68$. Hence from Corollary 3, we get $k \leqslant 102$. Thus $\kappa = 102$ if $d = p^{\alpha}$.

We give another example $d = 5p^{\alpha}$. Then $\chi_1 = 5, \epsilon_0 = \epsilon_1 = \epsilon_2 = 1$. By Lemma 12(ii), we have $d < 25(k-1)$. Assume that $k \geqslant 38$. Then we observe that $k$ satisfies the assumption of Lemma 8(b). Now (8.5) if $d < 15(k-1)$ and (8.6) if $15(k-1) \leqslant d < 25(k-1)$ hold by Lemma 12(iii) and (iv). Therefore $\delta \leqslant \frac{1}{2} + 65/(4k)$. Hence from Corollary 3, we get $k \leqslant 54$. Thus $\kappa = 54$ if $d = 5p^{\alpha}$. The value of $\kappa$ in all other cases is obtained similarly implying (8.7). □

Lemma 13 is proved under the assumption that $k-1$ is prime. If it is not satisfied, we can take $\kappa = \max(\nu_2', 160)$. This is clear from the proofs of our lemmas.

## 9. An Algorithm for Solving (2.11) with all Variables Bounded

We shall assume (2.11) with $P(b) < k$. By Lemma 13, there are only finitely many possibilities for $k$. Let $k = k_0$. By Lemma 12, we see that $n$ and $d$ are bounded by numbers depending only on $k_0$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\alpha_5$ be positive numbers depending only on $k_0$. Let $n + (k_0 - 1)d \leqslant \alpha_1$ and $\alpha_2 \leqslant d \leqslant \alpha_3$. We give an algorithm for finding possible solutions of (2.11) with $k = k_0$ and we shall always suppose that $k_0 \geqslant 6$ while applying this algorithm. This algorithm depends on Lemma 12 and Corollary 3. Therefore it is efficient only when $\omega(d)$ is small.

*Step 1.* Let $\alpha_4$ be given by Lemma 6 satisfying $n + (k_0 - 1)d \geqslant \alpha_4$. Then $n \geqslant \alpha_4 - (k_0 - 1)\alpha_3$ and we use (4.2) to find a lower bound for $|S_1|$. Further we use the argument in the begining of Lemma 6(ii) with $g_1 = q_1^2(k_0)/k_0^3$ by (2.14) to obtain another lower bound for $|S_1|$. We also recall that $|S_1| \geqslant 1$. Now we take $\alpha_5$ to be the maximum of the three lower bounds given above for $|S_1|$. We conclude that there is a term on the left hand side of (2.11) divisible by a prime $Q_0 \geqslant p_{\pi(k_0-1)+\alpha_5}$ to an even power. Thus it is of the form $t_0 Q_0^2$ where $t_0$ is a positive integer. We compute all primes $Q$ such that $p_{\pi(k_0-1)+\alpha_5} \leqslant Q \leqslant \sqrt{\alpha_1}$. Let $d$ be fixed with $\alpha_2 \leqslant d \leqslant \alpha_3$. For each $Q$ we form the set

$$D_Q = \{tQ^2 \mid \gcd(tQ^2, d) = 1, \max(\alpha_4 - (k_0 - 1)d, 2) \leqslant tQ^2 \leqslant \alpha_1\}.$$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

We observe that Lemma 12 and Corollary 3 provide a good upper bound for $|D_Q|$. We put $\mathcal{E}_d = \bigcup D_Q$ where the union is taken over all $Q$ satisfying $p_{\pi(k_0-1)+\alpha_5} \leqslant Q \leqslant \sqrt{\alpha_1}$. Thus $\mathcal{E}_d$ contains a term from the left-hand side of (2.11).

*Step 2*. Suppose $N \in \mathcal{E}_d$. For a positive integer $i$, we say that the property $P_{+\mathrm{id}}$ holds for $N$ if $r_1 = P(N + \mathrm{id}) \geqslant k_0$ such that $\mathrm{ord}_{r_1}(N + \mathrm{id}) \equiv 1 (\mathrm{mod}\ 2)$ and property $P_{-\mathrm{id}}$ holds for $N$ if $r_2 = P(N - \mathrm{id}) \geqslant k_0$ such that $\mathrm{ord}_{r_2}(N - \mathrm{id}) \equiv 1\ (\mathrm{mod}\ 2)$. Finally, we say that the property $P_{\pm\mathrm{id}}$ holds for $N$ if both the properties $P_{+\mathrm{id}}$ and $P_{-\mathrm{id}}$ hold. Let $E_1$ be the set of those $N \in \mathcal{E}_d$ for which $P_{\pm d}$ holds and $E_2$ be the set of those $N \in \mathcal{E}_d$ for which $P_{\pm 2d}$ holds. Let $E_1^c$ and $E_2^c$ denote the complements of $E_1$ and $E_2$ in $\mathcal{E}_d$, respectively. Put $\mathcal{E}_{d,1} = E_1^c \bigcup E_2^c$. We write $\mathcal{E}_{d,1} = X_1 + Y_1$ where $X_1$ and $Y_1$ are disjoint subsets of $\mathcal{E}_{d,1}$ given by $X_1 = E_1^c \bigcup E_2^c - (E_1^c \cap E_2^c)$ and $Y_1 = E_1^c \cap E_2^c$. Let $E_3$ be the set of $N \in \mathcal{E}_{d,1}$ for which $P_{\pm 3d}$ holds. Then we form $\mathcal{E}_{d,2} = X_2 + Y_2$ where $X_2 = X_1 - E_3 \cap X_1 + E_3 \cap Y_1$ and $Y_2 = Y_1 - E_3 \cap Y_1$ are disjoint. Now we proceed inductively to form the sets

$$\mathcal{E}_d \supseteq \mathcal{E}_{d,1} \supseteq \mathcal{E}_{d,2} \supseteq \mathcal{E}_{d,3} \supseteq \cdots$$

such that for $i \geqslant 2$, $\mathcal{E}_{d,i} = X_i + Y_i$ where

$$X_i = X_{i-1} - E_{i+1} \cap X_{i-1} + E_{i+1} \cap Y_{i-1},\ Y_i = Y_{i-1} - E_{i+1} \cap Y_{i-1}$$

and $E_{i+1}$ is the set of $N \in \mathcal{E}_{d,i-1}$ for which $P_{\pm(i+1)d}$ holds.

*Step 3*. We construct the sequence $\mathcal{E}_d, \mathcal{E}_{d,1}, \mathcal{E}_{d,2}, \mathcal{E}_{d,3}, \ldots$ for every $d$ with $\alpha_2 \leqslant d \leqslant \alpha_3$.

LEMMA 14. *If* $\mathcal{E}_{d,i} = \phi$ *for some* $i$ *with* $1 \leqslant i \leqslant [k_0/2] - 1$, *then* (2.11) *has no solution with* $k = k_0$.

*Proof*. Let $N \in \mathcal{E}_d$ such that $N$ is a term from the left-hand side of (2.11). Such a $N$ exists as already pointed out. Suppose $\mathcal{E}_{d,i} = \phi$ for some $i$ with $1 \leqslant i \leqslant [k_0/2] - 1$. Then by the construction of $\mathcal{E}_{d,i}$'s, we find that there exist integers $m_1$, $m_2$ with $1 \leqslant m_1 < m_2 \leqslant i + 1 \leqslant [k_0/2]$ such that $P_{\pm m_1 d}$ and $P_{\pm m_2 d}$ hold for $N$. Let $N = n + \mu d$ with $0 \leqslant \mu \leqslant [k_0/2] - 1$. Then $N + m_1 d$ and $N + m_2 d$ are $\leqslant n + (k_0 - 1)d$ and since at most one term in the product $n(n + d) \cdots (n + (k - 1)d)$ is omitted, there is a term in the product which equals $N + i_1 d$ with $i_1 = m_1$ or $m_2$ and $P_{i_1 d}$ holds. This is a contradiction. Let $N = n + \mu d$ with $[k_0/2] \leqslant \mu \leqslant k_0 - 1$. Then $N - m_1 d$ and $N - m_2 d$ are $\geqslant n$ and we obtain the contradiction as above. □

If the hypothesis of Lemma 14 is not satisfied (and this is the case for small values of $k$), we check directly that there is a term in the left-hand side of (2.11) which is divisible by a prime $\geqslant k_0$ to an odd power.

LEMMA 15. *Suppose that* $k$ *satisfies the assumptions stated in the begining of Section* 7. *Also let* $k - 1$ *be prime if* $k \geqslant 12$. *Then* (2.11) *with* $P(b) < k$ *does not hold.*

*Proof*. By Lemmas 12 and 13, the bounds for $n, d, k$ are given by (8.1)–(8.7). We make use of the algorithm described above to prove the assertion of the lemma. We illustrate with two examples. First we consider the case $d = p^\alpha$. Then $k \leqslant 102$ by (8.7). Further we take $k = 102$. In the notation of the algorithm, we fix $k = k_0 = 102$. By (8.5) and (8.2), we get $n + (k_0 - 1)d \leqslant 564417$, $d \leqslant 3(k_0 - 1)$. On the other hand, by Lemma 6, we get $n + (k_0 - 1)d > .52k_0^3$. Thus we have

$$\alpha_1 = 564417, \qquad \alpha_2 = 3, \qquad \alpha_3 = 293, \qquad \alpha_4 = 551828 \quad \text{and} \quad n \geqslant 522235.$$

We follow the procedure in Step 1 to get $|S_1| \geqslant 39$. Thus $\alpha_5 = 39$. We fix $d = 293$. Then $313 \leqslant Q \leqslant 751$. Suppose $Q = 751$. Then $D_Q = \{564001\}$. For each $Q$, we form the set $D_Q$ and we obtain

$$\begin{aligned}\mathcal{E}_d = \bigcup D_Q = &\{528529, 531723, 537289, 538756, 542882, 546121, 547058,\\ &547805, 552049, 556516, 557283, 562467, 564001\}.\end{aligned}$$

Now we follow Step 2. We find $\mathcal{E}_{d,1} = \{556516, 573049\}$ and $\mathcal{E}_{d,2} = \phi$. Hence, by Lemma 14, we find that (2.11) has no solution with $k = 102$ and $d = 293$. Similarly we exclude all values of $d$. We proceed like this to show that (2.11) has no solution for all $k$ with $68 \leqslant k < 102$ and $k - 1$ prime. Now let $k \leqslant 62$. We fix $k = k_0 = 62$. By (8.1), (8.4) and Lemma 6, we get $\alpha_1 = 254665, \alpha_2 = 3, \alpha_3 = 243, \alpha_4 = 94068$, $\alpha_5 = 20$. We fix $d = 243$. Now we apply the algorithm as earlier. We find that $\mathcal{E}_d$ has 90 elements and $\mathcal{E}_{d,3} = \phi$. We apply Lemma 14 to derive that (2.11) has no solution for $k = 62$. All other values of $k < 62$ with $k - 1$ prime are excluded similarly. This completes the proof of Lemma 15 when $d = p^\alpha$.

Next we explain the case $d = 5p^\alpha$. Then $\chi_1 = 5, \epsilon_0 = \epsilon_1 = \epsilon_2 = 1$. By (8.7) and (8.3), we have

$$k \leqslant 54, \;\; d < 25(k - 1). \tag{9.1}$$

We fix $k = k_0 = 54$. By Lemma 6, we get $n + (k_0 - 1)d \geqslant .6599\, k_0^3$. Let $d < 15(k_0 - 1)$. Then (8.5) is valid since $k$ satisfies the assumption of Lemma 8(b). Thus $n + (k_0 - 1)d \leqslant 126117$. Further we have $\alpha_1 = 126117, \alpha_2 = 35, \alpha_3 = 785$, $\alpha_4 = 103910$. Also $n \geqslant \alpha_4 - 53\,\alpha_3 = 62305$. By Step 1, we get $|S_1| \geqslant 20$. Thus $\alpha_5 = 20$. We fix $d = 785$. Then $151 \leqslant Q \leqslant 353$. Suppose $Q = 353$. Then $D_Q = \{124609\}$. For each $Q$, we compute $D_Q$ and form $\mathcal{E}_d$. We find that $\mathcal{E}_d$ contains 46 elements. Now we follow Step 2. We find

$$\mathcal{E}_{d,1} = \{69169, 72361, 74498, 85849, 98283, 99458, 108578, 113569, 124609\}$$

and $\mathcal{E}_{d,2} = \phi$. Hence, we conclude from Lemma 14 that (2.11) has no solution with $k = 54, d = 785$. Similarly we exclude all values of $d$ with $35 \leqslant d < 785$. Thus we may suppose by (9.1) that $15(k_0 - 1) \leqslant d < 25(k_0 - 1)$. Then by (8.6), we get $n + (k_0 - 1)d \leqslant 91125$. On the other hand, $n + (k_0 - 1)d \geqslant 103910$ by Lemma 6. This is a contradiction. Thus (2.11) has no solution with $k = 54$. We proceed like this to exclude all values of $k$ with $38 \leqslant k < 54$ such that $k - 1$ is prime. Let $12 \leqslant k < 38$. We fix $k = k_0 = 32$. By Lemma 6, we get $n + (k_0 - 1)d \geqslant .0417k_0^3$. Let $d < 20(k_0 - 1)$. Then by (8.4), we get $n + (k_0 - 1)d \leqslant 54528$. Thus we have

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

$\alpha_1 = 54528, \alpha_2 = 35, \alpha_3 = 605, \alpha_4 = 1366, \alpha_5 = 8$. We fix $d = 605$. We find that $\mathcal{E}_d$ contains 98 elements and $\mathcal{E}_{d,3} = \phi$. Hence, (2.11) has no solution with $k = 32, d = 605$. Similarly we exclude all values of $d$. Thus we may suppose that $20(k_0 - 1) \leqslant d < 25(k_0 - 1)$. By (8.6), we get $n + (k_0 - 1)d \leqslant 32000$. Thus $\alpha_1 = 32000, \alpha_2 = 635, \alpha_3 = 755, \alpha_4 = 1366, \alpha_5 = 8$. We fix $d = 755$. We find that $\mathcal{E}_d$ contains 45 elements and $\mathcal{E}_{d,3} = \phi$. Hence (2.11) has no solution with $k = 32, d = 755$. Similarly we exclude all values of $d$. Thus (2.11) has no solution with $k = 32$. Likewise we exclude all values of $k$ with $12 \leqslant k < 32$ and $k - 1$ prime. The proof for other values of $d \neq p^\alpha, 5p^\alpha$ is similar. $\square$

## 10. The Assumption $k-1$ Prime if $k \geqslant 12$ and the Final Lemma

For removing the assumption that $k - 1$ is prime if $k \geqslant 12$ in Lemma 15 we prove the following result which is true for any $d$.

LEMMA 16. *Let* $\varphi \in \{0, 1\}$ *and* $d$ *be given. Let* $k_1 < k_2$ *be positive integers such that* $k_1 - 1$ *and* $k_2 - 1$ *are consecutive primes. Suppose that* (2.11) *with* $k = k_1$ *and* $t = k_1 - \varphi$ *has no solution in integers* $n, d_1, \ldots, d_t$ *and* $b$ *with* $n > 0, d_i \in [0, k_1)$ *for* $1 \leqslant i \leqslant t$ *and* $P(b) < k_1$. *Let* $k_1 < k_2$. *Then* (2.11) *with* $k = k', t = k' - \varphi$ *and* $P(b) < k'$ *does not hold.*

*Proof.* Let $\varphi \in \{0, 1\}$ and $d$ be given. Suppose (2.11) holds for some $k = k'$ with $k_1 < k' < k_2, t = k' - \varphi$ and $P(b) < k'$. We see that $k' - 1$ is not a prime. Hence $P(b) < k' - 1$ and each term $n + d_i d = a_i x_i^2$ satisfies $P(a_i) < k' - 1$ such that

$$(n + d_1 d) \cdots (n + d_{t-1} d) = b' y^2 \tag{10.1}$$

with $P(b') < k' - 1$. If $k' - 1 = k_1$, then by our hypothesis, (10.1) has no solution and hence (2.11) with $k = k', t = k' - \varphi$ and $P(b) < k'$ has no solution. If $k' - 1 > k_1$, then $k' - 2$ is not a prime and arguing as before from (10.1), we get

$$(n + d_1 d) \ldots (n + d_{t-2} d) = b'' y^2$$

with $P(b'') < k' - 2$ and we proceed inductively to see that the assertion of the lemma holds. If $\varphi = 1$ we continue to be in the case $\varphi = 1$ throughout the induction process. This is clear when $n$ is the omitted term. For securing this when $n$ is not an omitted term, we regard $n(n + d) \cdots (n + id)$ as a product from $n(n + d) \cdots (n + (i + 1)d)$ with $n + (i + 1)d$ as an omitted term. $\square$

We combine Lemmas 15 and 16 to conclude the following result.

LEMMA 17. *Assume* (2.11) *with* $P(b) < k$ *and* $k \geqslant 4$. *Then* $k \leqslant 9$ *and* $b > 1$ *if* $d = p^\alpha$, $t = k$; $k \leqslant 29$ *if* $d = p^\alpha, t = k - 1$ *and* $k \leqslant 11$ *otherwise.*

*Proof.* We assume (2.11) with $P(b) < k$ with $k \geqslant 4$. Then we derive that $b > 1$ if $k = 4, 5$ and $t = k$ by the results of Euler and Obláth stated in Section 1. Further, we may suppose that $k$ satisfies the assumptions stated in the begining of Section 7. By Lemma 16, there is no loss of generality in assuming that $k - 1$ is prime for $k \geqslant 12$. Finally we apply Lemma 15 to arrive at a contradiction. $\square$

## 11. Proofs of the Theorems and Corollaries

From Lemma 17, we derive

COROLLARY 4. *Assume* (1.1) *with* $\gcd(n, d) = 1$ *and* $P(b) < k$.

(i) *If* $d = p^\alpha, b = 1$, *then* $k = 3$.
(ii) *If* $d = p^\alpha$, *then* $k \leqslant 9$.
(iii) *If* $d \neq p^\alpha$, *then either* $k = 3, d = 7p^\alpha$ *or* $(n, d, k) = (1, 24, 3)$.

*Proof*. Assume (1.1) with $\gcd(n, d) = 1$ and $P(b) < k$. Then (2.11) with $t = k$ and $P(b) < k$ holds. Now (i) and (ii) follow directly from Lemma 17 and (iii) is obtained by combining Lemmas 17 and 2. □

*Proof of Theorem* 4. By Lemma 17, we may assume that $d \neq p^\alpha$, $k \leqslant 11$ and the assertion follows from Lemma 2. □

*Proof of Theorem* 3. Assume (1.1) with $\gcd(n, d) = 1$ and $P(b) = k$. Further we may assume that $k \geqslant 30$ if $d = p^\alpha$. Also we see from Lemma 2 that $k \geqslant 12$ if $d \neq p^\alpha$. We delete the term divisible by $k$ on the left-hand side of (1.1). By Corollary 4, we may suppose that the deleted term is neither $n$ nor $n + (k-1)d$. Hence (1.3) is valid with $0 < i < k-1$. This is not possible by Theorem 4. □

*Proof of Corollary* 1. Assume (1.1) with $\gcd(n, d) = 1$ and $1 < d \leqslant 104$. Then $d \in \mathcal{D}$. Let $d \in \{p^\alpha, 7p^\alpha\}, k = 3$. Now (1.1) can be written as

$$Y^2 + a_1' XY + a_3' Y = X^3 + a_2' X^2 + a_4' X + a_6',$$

where $X = b(n+d)$, $Y = b^2 y$, $a_1' = a_2' = a_3' = a_6' = 0$, $a_4' = -b^2 d^2$. Thus we have

$$Y^2 = X^3 - b^2 d^2 X \tag{11.1}$$

with $X$ and $Y$ as above. The cases

$$d = 17, 103 \quad \text{and} \quad b = 1; d = 61, 101 \quad \text{and} \quad b = 3; \quad d = 25 \quad \text{and} \quad b = 6$$

are excluded by congruence considerations. In the remaining cases we compute all the integral solutions $(X, Y)$ of the above elliptic equation using SIMATH from which we find that the solutions of (1.1) are given by

$$\begin{aligned}(n, d) \in \{&(2, 7), (18, 7), (64, 17), (2, 23), (4, 23), (75, 23), (98, 23), (338, 23),\\ &(3675, 23), (800, 41), (2, 47), (27, 71), (50, 71), (96, 73), (864, 97)\}.\end{aligned} \tag{11.2}$$

Further, for $d \neq p^\alpha, 7p^\alpha$ and $k = 3$, we see that $(n, d) = (1, 24)$ by Lemma 2. Suppose $d = p^\alpha, k = 4$. Then (1.1) with $d = p^\alpha, k = 3$ holds and by (11.2) we see that $(n, d) = (75, 23)$. Next let $d = p^\alpha, k = 5$. Then we may assume that $5 \mid a_2$ otherwise the assertion follows from (11.2) as above. We see that $a_0, a_1, a_3, a_4 \in \{1, 2, 3, 6\}$ and by using Legendre Symbol mod 5 we have either $a_0, a_4 \in \{1, 6\}, a_1, a_3 \in \{2, 3\}$

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

or $a_0, a_4 \in \{2, 3\}, a_1, a_3 \in \{1, 6\}$. Hence, $a_0 = a_4 = 1$ with $x_0, x_4$ odd or $a_1 = a_3 = 1$ with $x_1, x_3$ odd. This is not possible by (3.1). Thus we may assume that $k \geqslant 6$ whenever $d = p^\alpha$. By Corollary 4 and Theorem 3 we need to consider only

$$d = p^\alpha \text{ with } 6 \leqslant k \leqslant 9 \quad \text{or if } k \text{ is prime, } 11 \leqslant k \leqslant 29. \tag{11.3}$$

Let $|R| \geqslant k-1$. By (2.15), we see that $(n/p) = (a_i/p)$ for $0 \leqslant i < k$. Further, $f(2) \geqslant 3$. Therefore $p \neq 3$ and $(2/p) = (3/p) = 1$ which implies that $d = 23, 47, 71, 73, 97$. Further, we may assume that $P(a_{i_0}) = 5$ for some $i_0$ with $0 \leqslant i_0 < k$. Thus $p \neq 5$ and $1 = (a_{i_0}/p) = (5/p)$. On the other hand, we observe that $(5/p) = -1$ for $p = 23, 47, 73, 97$. This is a contradiction implying that $d = 71$. For $k \geqslant 8$, there exists $i_1$ such that $P(a_{i_1}) = 7$ and $1 = (a_{i_1}/71) = (7/71) = -1$, a contradiction. Thus $k = 6, 7$. Since $f(2) \geqslant 3$, there exist nonnegative integers $i', i$ and $j$ with $i > 0$ and $i' + i < i' + j \leqslant k-1$ such that

$$X'(X' + id)(X' + jd) = b_1 y_1^2 \tag{11.4}$$

where $X' = n + i'd$, and $b_1, y_1$ are positive integers with $P(b_1) \leqslant 3$. We may assume that gcd $(X', i, j, b_1) = 1$. We rewrite the above equation as

$$X(X + ib_1 d)(X + jb_1 d) = Y^2$$

where $X = b_1 X'$, $Y = b_1^2 y_1$. Then we use SIMATH to find all the solutions of the above elliptic curve and we conclude that (1.1) with $d = 71$ has no solution.

Let $|R| \leqslant k-2$. Suppose (a) and (b) of Lemma 9 do not hold. Arguing as in Lemma 11(i), we see that there exist distinct $\mu_0, \nu_0 \in R_1^{(2)}$ and $\mu_1, \nu_1$ with $\mu_0 > \mu_1, \nu_0 > \nu_1$ satisfying (7.5) and $(h_1, h_2) = (1, p^\alpha)$ is the partition corresponding to both $a_{\mu_0} = a_{\mu_1}$ and $a_{\nu_0} = a_{\nu_1}$. Further, (7.6) holds with $c = 1$. Hence, we conclude from Lemma 10 that

$$n < (k-1)^2 \min\left(\frac{d}{4}, k - \frac{3}{4}\right), \quad d < 4(k-1). \tag{11.5}$$

Suppose (a) or (b) of Lemma 9 holds. Then (7.1) is valid which gives (11.5). Thus (11.5) is always valid. Now we apply the algorithm of Section 9 after replacing $P(b) < k$ by $P(b) \leqslant k$ and the values of $n, d, k$ given by (11.5), (11.3) are excluded. $\square$

*Proof of Corollary* 2. We shall use (11.4) several times with the assumption on $b_1$ relaxed to $P(b_1) \leqslant 5$. We denote by $b_2, \ldots, b_5$ and $y_2, \ldots, y_5$ positive integers such that $P(b_i) \leqslant 5$. Assume (1.3) with $\gcd(n, d) = 1$ and $P(b) < k$. By Theorem 4, we need to consider only

$$k \leqslant 29, d = p^\alpha; k = 4, 5, d = 35, 45, 55, 63, 65. \tag{11.6}$$

The following cases of (11.4) are solved by congruence considerations in addition to the ones stated in the begining of the proof of Corollary 1:

$b_1 = 2, d = 25$ or $b_1 = 1, d = 61$ if $i = 1, j = 3$;
$b_1 = 3, d = 25$ or $b_1 = 2, d = 43$ or $b_1 = 2, d = 53$ if $i = 2, j = 3$;
$b_1 = 30, d = 59$ or $b_1 = 15, d = 67$ or $b_1 = 5, d = 67$ if $i = 1, j = 2$.

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

It will be assumed in the subsequent argument without reference that the above cases are already solved.

Let $k = 4, 5$. Then we find that an equation of the form (11.4) with $P(b_1) \leqslant 3$ is valid. Now we use SIMATH as in Corollary 1 to find all the solutions of (1.3). Thus we assume that $k \geqslant 6$. Then $d = p^\alpha$ by (11.6). We shall again use SIMATH in the remaining part of the proof without reference for solving elliptic equations in integers.

First we consider the case $|R| \geqslant k - 2$. Then we see that $p \neq 3$ from $f(2) \geqslant 2$ and $(\frac{1}{3}) \neq (\frac{2}{3})$. Let $k \geqslant 9$. Then $f(2) \geqslant 3$ which implies that $(2/p) = (3/p) = 1$. Thus $d = 23, 47$. But there exists $i_0$ with $0 \leqslant i_0 < k$ such that $P(a_{i_0}) = 5$. Hence $1 = (a_{i_0}/p) = (5/p) = -1$ for $p = 23, 47$ a contradiction. Thus we conclude that $k \leqslant 8$. Let $k = 6$ or 7. Then we see that either

$$n(n + d)(n + 2d) = b_2 y_2^2$$

or

$$(n + 3d)(n + 4d)(n + 5d) = b_3 y_3^2.$$

Thus (11.1) is valid with $b = b_2, X = b_2(n + d), Y = b_2^2 y_2$ or with $b = b_3, X = b_3(n + 4d), Y = b_3^2 y_3$. Now we compute all the integral solutions of these elliptic equations from which we see that (1.3) has the only solution $(n, d, k) = (5, 11, 6)$.

Let $k = 8$. Suppose 7 divides $a_0$ and $a_7$. Then

$$(n + id)(n + (i + 1)d)(n + (i + 2)d) = b_4 y_4^2 \tag{11.7}$$

with $i = 1$ holds. Hence (11.1) is valid with $b = b_4, X = b_4(n + 2d), Y = b_4^2 y_4$. By computing all the integral solutions of these elliptic equations we see that (1.3) has no solution. Suppose 7 divides only one $a_i$. Then (11.7) holds for some $i$ with $0 \leqslant i \leqslant 5$ or $7 \mid a_2$ and $n + 5d$ is omitted or $7 \mid a_5$ and $n + 2d$ is omitted. The first possibility is excluded as earlier. In the latter two possibilities we see that (11.4) holds with $X' = n, y_1 = y_5, b_1 = b_5, i = 1, j = 3$. Now we compute all the integral solutions of these elliptic equations from which we find that (1.3) has no solution.

Suppose $|R| \leqslant k - 3$. Then as seen in Corollary 1, (11.5) holds. Further the values of $n, d, k$ given by (11.5) and $k \leqslant 29, d = p^\alpha$ are excluded by using the algorithm of Section 9. □

*Proof of Theorem* 2. We denote by $b_6, b_7, b_8$ and $y_6, y_7, y_8$ positive integers such that $P(b_i) < k$. Let the assumptions of Theorem 2 be satisfied. We may assume that $k \geqslant 4$. By Corollary 4(iii), we may suppose that $\gcd(n, d) > 1$. Further we divide both the sides of (1.1) by $\gcd(n, \chi)$ to observe that there is no loss of generality in assuming that $\gcd(n, \chi) = 1$. For the preceding observation we assume that the second possibility in the assertion of Theorem 2 is excluded. We observe that $\chi > 1$ unless $d = 2^\alpha$. Further $\gcd(n, d) = \tau^\beta, \beta > 0$. Let $n' = n/\tau^\beta$ and $d' = d/\tau^\beta = \chi\tau^{\alpha-\beta.}$

Then (1.1) becomes

$$\tau^{\beta k} n'(n'+d')\dots(n'+(k-1)d') = by^2 \tag{11.8}$$

with $\gcd(n', d') = 1$.

Let $\alpha - \beta > 0$. If $\tau \geqslant k$, we observe that $\beta k$ is even and we derive from (11.8) that

$$n'(n'+d')\dots(n'+(k-1)d') = b_6 y_6^2. \tag{11.9}$$

Further (11.9) follows from (11.8) when $\tau < k$. Thus (11.9) is always valid. On the other hand, (11.9) is not possible by $\chi > 1$ if $d \neq 2^\alpha$ and Corollary 4(iii).

Thus we may assume that $\alpha - \beta = 0$. Then $d \neq 2^\alpha$ since $d \nmid n$. Therefore $\chi > 1$. From (11.8) we get either

$$n'(n'+\chi)\cdots(n'+(k-1)\chi) = b_7 y_7^2 \tag{11.10}$$

or $\tau = p \geqslant k$, $\alpha k$ odd and

$$n'(n'+\chi)\cdots(n'+(k-1)\chi) = pb_8 y_8^2. \tag{11.11}$$

We exclude (11.10) by Corollary 1 since $\chi \leqslant 12$. Suppose that (11.11) holds. Then $k \geqslant 5$ and $k \neq 6$. We omit the term divisible by $p$ on the left-hand side of (11.11). We may suppose that the omitted term is neither $n'$ nor $n' + (k-1)\chi$ since otherwise the assertion follows from Corollary 1. Now we apply Corollary 2 to (11.11) to get $(n', \chi, p, k) =$ (4, 7, 11, 5). This implies that $(n, d, k) = (4 \cdot 11^\alpha, 7 \cdot 11^\alpha, 5)$ with $\alpha$ odd. □

*Proof of Theorem* 1. We assume (1.1) with $d = \tau^\alpha$ where $\tau = p, k \geqslant 4, P(b) < k$. We may suppose that $\gcd(n, d) > 1$ by Corollary 4(i),(ii). Let $\beta = \min(\mathrm{ord}_p(n), \alpha)$, $n' = n/p^\beta, d' = d/p^\beta$. Thus $\gcd(n', d') = 1$ and (11.8) is valid.

(i) Suppose $b = 1$. Let $\mathrm{ord}_p(n) \neq \alpha$. Then the order of $p$ dividing the left hand side of (11.8) is $\beta k$ and it is even. This is not possible by Corollary 4(i) and a result of Erdős [2] and Rigge [8] proved independently that a product of two or more consecutive positive integers is not a square. Thus $\mathrm{ord}_p(n) = \alpha$ and we re-write (11.8) as

$$p^{\alpha k} n'(n'+1)\cdots(n'+k-1) = y^2. \tag{11.12}$$

Further, we may suppose as above that $k$ is odd. Let $n' > k$. We see from [13, Corollary 3(ii)] that $n'(n'+1)\dots(n'+k-1)$ is divisible by at least two distinct primes exceeding $k$ unless $n' = 6, 8$ and $k = 5$. The latter possibilities are excluded by (11.12) and we conclude from (11.12) that $n' > k^2$. Now, as stated in Section 1 on (1.1) with $d = 1$, we derive that $n'(n'+1)\cdots(n'+k-1)$ is divisible by at least two distinct primes exceeding $k$ to odd powers. This contradicts (11.12). Hence, we conclude that $n' \leqslant k$. If $n' + k \leqslant 12$, we check directly that (11.12) is not valid. Thus we may assume $n' + k > 12$. Further $n' \leqslant (n'+k)/2 < n' + k - 1$ and $\pi(n'+k-1) - \pi((n'+k)/2) \geqslant 2$. Thus the left hand side of (11.12) is divisible by a prime exactly to the first power. This is not possible.

(ii) Let $b > 1$ and $d \nmid n$. Then $d' > 1$ and $\mathrm{ord}_p(n) \neq \alpha$. Then we observe as above from (11.8) that $\beta k$ is even if $p \geqslant k$ and we derive (11.9). Now we apply Corollary 4(ii) to (11.9) for getting $k \leqslant 9$. □

https://doi.org/10.1023/A:1025408727362 Published online by Cambridge University Press

## Acknowledgement

We thank the referee for his comments and remarks on an earlier draft of the paper. These led to a considerable improvement in the exposition of the paper.


## References


1. Dickson, L. E.: *History of the Theory of Numbers*, *Vol* II, Chelsea Publ. Co., 1952.
2. Erdős, P.: Note on the product of consecutive integers (II), *J. London Math. Soc.* **14** (939), 245–249.
3. Erdős, P. and Selfridge, J. L.: The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301.
4. Filakovszky, P. and Hajdu, L.: The resolution of the diophantine equation $x(x+d)\dots(x+(k-1)d) = by^2$ for fixed $d$, *Acta Arith.* **98** (2001), 151–154.
5. Marszalek, R.: On the product of consecutive elements of an arithmetic progression, *Monatsh. Math.* **100** (1985), 215–222.
6. Mordell, L. J.: *Diophantine Equations*, Academic Press, New York, 1969.
7. Obláth, R.: Über das produkt funf aufeinander folgender zahlen in einer arithmetischen reihe, *Publ. Math. Debrecen* **1** (1950), 222–226.
8. Rigge, O.: Über ein diophantisches problem, In: *9th Congress Math. Scand., Helsingfors, 1938*, Mercator, 1939, pp. 155–160.
9. Rosser, B. and Schoenfeld, L.: Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.
10. Saradha, N.: On perfect powers in products with terms from arithmetic progressions, *Acta Arith.* **82** (1997), 147–172.
11. Saradha, N.: Squares in products with terms in an arithmetic progression, *Acta Arith.* **86** (1998), 27–43.
12. Saradha, N. and Shorey, T. N.: Almost perfect powers in arithmetic progression, *Acta Arith.* **99** (2001), 363–388.
13. Saradha, N. and Shorey, T. N.: Almost squares and factorisations in consecutive integers, *Compositio Math.* **138** (2003), 113–124.
14. Shorey, T. N.: Exponential diophantine equations involving products of consecutive integers and related equations, In: R. P. Bambah, V. C. Dumir and R. J. Hans-Gill (eds), *Number Theory*, Hindustan Book Agency, 1999, pp. 463–495.
15. Shorey, T. N.: Powers in arithmetic progression, In: G. Wüstholz (ed.), *A Panorama in Number Theory or The View from Baker's Garden*, Cambridge Univ. Press, 2002, pp. 325–336.
16. Shorey, T. N. and Tijdeman, R.: Perfect powers in products of terms in an arithmetical progression, *Compositio Math.* **75** (1990), 307–344.
17. Shorey, T. N. and Tijdeman, R.: On the greatest prime factor of an arithmetical progression, In: A. Baker, B. Bollobás and A. Hajnal (eds), *A Tribute to Paul Erdős*, Cambridge Univ. Press, 1990, pp. 385–389.
18. Shorey, T. N. and Tijdeman, R.: Some methods of Erdös applied to finite arithmetic progressions, In: R. L. Graham and J. Nesetril (eds), *The Mathematics of Paul Erdős*, Springer, New York, 1997, pp. 251–267.