Some Topics in Number Theory
(Refinements, Extensions and Generalisations of a Theorem of Sylvester on the prime factors of a product of consecutive integers)

A Thesis

Submitted to the
Tata Institute of Fundamental Research, Mumbai
for the degree of Doctor of Philosophy
in Mathematics

by

Shanta Laishram

School of Mathematics,
Tata Institute of Fundamental Research,
Mumbai, India

April, 2007

DECLARATION

This thesis is a presentation of my original research work. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions.

The work was done under the guidance of Professor T. N. Shorey, at the Tata Institute of Fundamental Research, Mumbai.

Shanta Laishram

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

Professor T. N. Shorey
Date:

Acknowledgements

It is my great pleasure to express my heart-felt gratitude to all those who helped and encouraged me at various stages.

I am indebted to my advisor *Professor T. N. Shorey* for his invaluable guidance and constant support. His concern and encouragement have always comforted me throughout.

I would like to thank *Professors N. Saradha, E Ghate, C. S. Rajan and A. Sankaranarayanan* for introducing me to different topics in Number Theory.

I would like to thank *Professor Rob Tijdeman* for helpful discussions and encouragement.

I would like to thank *Professor Ravi Rao* for being always available for any kind of help and discussions. I would like to thank School of Mathematics staff for helping me in administrative matters and Dr Pablo and Mr Nandagopal for help in computer related matters.

My sincere thanks to *Dr H Jayantakumar and Professors M Ranjit and M. B. Rege* for their constant support and encouragements throughout since my school days.

Though one should not thank friends, I would like to mention *Ajay, Amala, Amit, Anand, Anoop, Anupam, Apoorva, Ashutosh, Arati, Chandrakant, Deepankar, Deepshikha, Ig, Meera, Rabeya, Rama Reddy, Ritumoni, Sarita, Shripad, Sriram, Umesh, Vaibhav, Vishal, Vivek* and others with whom I had spent a lot of time and for making my stay at TIFR lively and enjoyable one. I also really enjoyed the company and time I spent with many other research scholars in school of mathematics and other departments in TIFR.

I also cannot forget my friends outside TIFR whom I am in contact and whom I can always rely upon. My school and college friends like *Aken, Doren, Herachandra, Kebi, Marjit, Nirmal, Shekhar, Shanta and Suhesh* and other friends whom I met over the years like *Binod, Birendra, Debbie, Indrajit, Joykumar, Jugeshor, Kebi, Korou, Miranda, Nobin, Sarat, Shyam and Sanjoy.* Also I have been fortunate to meet quite a few frens while doing Mathematics like *Aaloka, Anisa, Arindam, Brundavan, Malapati, Purushottam, Rohit, Sanoli, Satadal, Sunayana, Swaralipy, Thyagaraju and Vikram.*

Finally, to *my parents Mahajon and Sanahanbi, my grandmother Angou, my brothers and sister and other relatives* who are always there for me and whom I cannot thank enough!

List of Publications

This thesis is based on the results of my publications listed here. All the papers have been either published or accepted for publication other than (ix) which has been submitted for publication. The results of (ix) are stated in Chapter 2(Section 2.6) and proved in Chapter 12. All other chapters of this thesis are independent of (ix).

(i) (with T. N. Shorey), *Number of prime divisors in a product of consecutive integers*, Acta Arith. **113** (2004), 327-341.

(ii) (with T. N. Shorey), *Number of prime divisors in a product of terms of an arithmetic progression*, Indag. Math., **15(4)** (2004), 505-521.

(iii) *An estimate for the length of an arithmetic progression the product of whose terms is almost square*, Pub. Math. Debrecen, **68** (2006), 451-475.

(iv) (with T. N. Shorey), *Greatest prime factor of a product of consecutive integers*, Acta Arith., **120** (2005), 299-306.

(v) (with T. N. Shorey), *The greatest prime divisor of a product of terms in an arithmetic progression*, Indag. Math., **17(3)** (2006), 425-436.

(vi) (with T. N. Shorey), *Grimm's Conjecture on consecutive integers*, Int. Jour. Number Theory, **2** (2006), 207-211.

(vii) (with Hirata-Kohno, T. N. Shorey and R. Tijdeman), *An extension of a theorem of Euler*, Acta Arith., accepted for publication.

$(viii)$ (with T. N. Shorey), *The equation* $n(n+d)\cdots(n+(k-1)d) = by^2$ *with* $\omega(d) \leq 6$ *or* $d \leq 10^{10}$, Acta Arith., accepted for publication.

(ix) (with T. N. Shorey), *Squares in products in arithmetic progression with at most two terms omitted and common difference a prime power*, submitted.

Contents

Introduction

An old and well known *theorem of Sylvester for consecutive integers* [**77**] states that *a product of k consecutive integers each of which exceeds k is divisible by a prime greater than k.*

In this thesis, we give refinements, extensions, generalisations and applications of the above theorem. First we give some notation which will be used throughout the thesis.

Let p_i denote the i-th prime number. Thus $p_1 = 2, p_2 = 3, \ldots$. We always write p for a prime number. For an integer $\nu > 1$, we denote by $\omega(\nu)$ and $P(\nu)$ the number of distinct prime divisors of ν and the greatest prime factor of ν, respectively. Further we put $\omega(1) = 0$ and $P(1) = 1$. For positive real number ν and positive integers l, a with $\gcd(l, a) = 1$, we denote

$$\pi(\nu) = \sum_{p \le \nu} 1,$$

$$\pi_a(\nu) = \sum_{\substack{p \le \nu \\ \gcd(p,a)=1}} 1,$$

$$\pi(\nu, a, l) = \sum_{\substack{p \le \nu \\ p \equiv l (\text{mod } a)}} 1.$$

We say that a number is *effectively computable* if it can be explicitly determined in terms of given parameters. We write *computable number* for an effectively computable number. Let $d \ge 1, k \ge 2, n \ge 1$ and $y \ge 1$ be integers with $\gcd(n, d) = 1$. We denote by

$$\Delta = \Delta(n, d, k) = n(n + d) \cdots (n + (k - 1)d)$$

and we write

$$\Delta(n, k) = \Delta(n, 1, k).$$

In the above notation, Sylvester's theorem can be stated as

$$P(\Delta(n, k)) > k \text{ if } n > k. \tag{1}$$

On the other hand, there are infinitely many pairs (n, k) with $n \le k$ such that $P(\Delta) \le k$. We notice that $\omega(\Delta(n, k)) \ge \pi(k)$ since $k!$ divides $\Delta(n, k)$. The first improvement in this direction is the following statement equivalent to (1)

$$\omega(\Delta(n, k)) > \pi(k) \text{ if } n > k. \tag{2}$$

Let $d > 1$. Sylvester [**77**] proved that

$$P(\Delta) > k \text{ if } \ n \ge k + d. \tag{3}$$

Langevin [**38**] improved (3) to

$$P(\Delta) > k \text{ if } n > k.$$

Finally Shorey and Tijdeman [**75**] proved that

$$P(\Delta) > k \ \text{ unless } \ (n, d, k) = (2, 7, 3). \tag{4}$$

We observe that it is necessary to exclude the triple $(2, 7, 3)$ in the above result since $P(2 \cdot 9 \cdot 16) = 3$.

We give a brief description of the thesis. The thesis is broadly divided into two parts. In Chapter 1, we give a survey on refinements and generalisations of Sylvester's Theorem. These include the statements of our new results and the proofs are given in Chapters $4 - 8$ in the Part 1 of the thesis.

In Chapter 2, we give a survey of results on the parity of power of primes greater than k dividing Δ including our new results which are proved in the Chapters $9-12$ in the Part 2 of the thesis. For proving these results, we require certain estimates on π function and other functions involving primes. In Chapter 3, we collect these results.

We begin with results stated in Chapter 1. First we consider results on the lower bound of $\omega(\Delta(n,k))$. Saradha and Shorey [**61**, Corollary 3] sharpened (2) by showing

$$\omega(\Delta(n,k)) \geq \pi(k) + \left[\frac{1}{3}\pi(k)\right] + 2 \text{ if } n > k \geq 3 \tag{5}$$

except when (n,k) belongs to an explicitly given finite set. This is best known for $3 \leq k \leq 18$. We improve $\frac{1}{3}$ in (5) to $\frac{3}{4}$ for $k \geq 19$. We have

Theorem 1. (Laishram and Shorey [**28**])

Let $k \geq 3$ and $n > k$. Then $\omega(\Delta(n,k)) \geq \pi(k) + [\frac{3}{4}\pi(k)] - 1$ except when (n,k) belongs to an explicitly given finite set.

A more precise statement including the exceptional set is given in Theorem 1.2.1 and a proof is given in Section 4.1. We observe that $\omega(\Delta(k+1,k)) = \pi(2k)$ and therefore, $\frac{3}{4}$ in Theorem 1 cannot be replaced by a number greater than 1. We refer to Theorem 1.2.4 and Corollary 1.2.5 for results in this regard.

An open conjecture of Grimm [**20**] states that *if $n, n+1, \cdots, n+k-1$ are all composite numbers, then there are distinct primes p_{i_j} such that $p_{i_j}|(n+j)$ for $0 \leq j < k$.* Erdős and Selfridge (see [**48**]) showed that Grimm's Conjecture implies that *there is a always a prime between two consecutive squares.* The latter result is out of bounds even after assuming Riemann hypothesis. Thus a proof of Grimm's Conjecture is very difficult. The best known result on Grimm's Conjecture is due to Ramachandra, Shorey and Tijdeman [**52**]. Grimm's Conjecture implies that if $n, n+1, \cdots, n+k-1$ are all composite, then $\omega(\Delta(n,k)) \geq k$ which is also open. In Chapter 5, we confirm Grimm's Conjecture for $n \leq 1.9 \times 10^{10}$ and for all k and as a consequence, we have

Theorem 2. (Laishram and Shorey, [**31**])

Assume that $n, \cdots, n+k-1$ are all composite and $n \leq 1.9 \times 10^{10}$. Then $\omega(\Delta(n,k)) \geq k$.

The next result is on a lower bound for $P(\Delta(n,k))$.

Theorem 3. (Laishram and Shorey [**30**])

We have

$$P(\Delta(n,k)) > 1.95k \text{ for } n > k > 2$$

unless (n,k) belongs to an explicitly given finite set.

We observe from $P(\Delta(k+1,k)) \leq 2k$ that 1.95 in Theorem 3 cannot be replaced by 2. Section 1.3 contains a more precise statement with an explicit list of the exceptions and some further results viz., Theorems 1.3.1, 1.3.3 and Corollary 1.3.2. A proof of these results are given in Chapter 6. Theorem 3 has been applied by Filaseta, Finch and Leidy [**18**] to prove irreducibility results for certain Generalised Laguerre polynominals over rationals. We refer to Section 1.3 for results in this regard. Now we turn to $d > 1$. We have the following result on $\omega(\Delta)$.

Theorem 4. (Laishram and Shorey [**29**])

Let $d > 1$. Then

$$\omega(\Delta(n,d,k)) \geq \pi(2k) - 1$$

except when $(n,d,k) = (1,3,10)$.

The above result is best possible for $d = 2$ since $\omega(1 \cdot 3 \cdots (2k-1)) = \pi(2k) - 1$. Theorem 4 solves a conjecture of Moree [**43**]. We refer to Section 1.4 on some more general results, particularly Theorem 1.4.1 from where Theorem 4 follows. We give a proof of Theorem 1.4.1 in Section 7.4.

On a lower bound for $P(\Delta)$, we have the following result.

Theorem 5. (Laishram and Shorey [**32**])

Let $d > 2$ and $k \geq 3$. Then

$$P(\Delta(n, d, k)) > 2k$$

unless (n, d, k) is given by given by an explicit finite set.

The case $d = 2$ for the inequality of Theorem 5 can be reduced to that of $d = 1$. A more precise statement with an explicit description of the exceptions is given in Theorem 1.5.1 and a proof is given in Chapter 8. The assertions of Theorem 1, 3 and 5 are not valid for the exceptions and therefore, it is necessary to exclude them.

Now we turn to Chapter 2 where we discuss the parity of power of primes greater than k dividing $\Delta(n, d, k)$. For this, we consider the equation

$$\Delta(n, d, k) = by^2. \tag{6}$$

with $P(b) \leq k$. In Chapter 9, we state the preliminaries and the general Lemmas for the proofs of the results stated in Chapter 2.

Let $d = 1$. It is a consequence of some old diophantine results that (6) with $k = 3$ is possible only when $n = 1, 2, 48$. Let $k \geq 4$. Erdős [**11**] and Rigge [**55**], independently, proved that product of two or more consecutive positive integers is never a square. More generally, Erdős and Selfridge [**13**] proved that (6) with $P(b) < k$ does not hold under the necessary assumption that the left hand side of (6) is divisible by a prime greater than or equal to k. The assumption $P(b) < k$ has been relaxed to $P(b) \leq k$ by Saradha [**60**] again under the necessary assumption that the left hand side of (6) is divisible by a prime exceeding k. We refer to Section 2.1 for details.

Therefore we suppose that $d > 1$. Let $k = 3$. There are infinitely many three squares in arithmetic progression and hence (6) has infinitely many solutions. Therefore we assume from now onwards that $k \geq 4$. Fermat (see Mordell [**42**, p.21]) showed that there are no four squares in an arithmetic progression. Euler ([**15**], cf. [**42**, p.21-22], [**43**]) proved a more general result that a product of four terms in arithmetic progression can never be a square. In Section 10.9, we prove the following extension of Euler's result.

Theorem 6. (Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**])

Equation (6) with $4 \leq k \leq 109$ and $b = 1$ is not possible.

The case $k = 5$ is due to Obláth [**50**]. Independently, Bennett, Bruin, Győry and Hajdu [**1**] proved Theorem 6 with $6 \leq k \leq 11$. A general conjecture states that Δ is divisible by a prime $> k$ to an odd power unless $k = 4, b = 6$. In other words,

Conjecture 1. *Equation (6) with $P(b) \leq k$ implies that $k = 4, b = 6$.*

A weaker version of Conjecture 1 is the following conjecture due to Erdős.

Conjecture 2. *Equation (6) with $P(b) \leq k$ implies k is bounded by a computable absolute constant.*

In Chapter 2, we give a survey of results on Conjectures 1 and 2.

We now consider Conjecture 1 with k fixed. Equation (6) with $k = 4$ and $b = 6$ has infinitely many solutions. On the other hand, (6) with $k = 4$ and $b \neq 6$ does not hold. Therefore we consider (6) with $k \geq 5$. We write

$$n + id = a_i x_i^2 \text{ for } 0 \leq i < k \tag{7}$$

where a_i are squarefree integers such that $P(a_i) \leq \max(P(b), k - 1)$ and x_i are positive integers. Every solution to (6) yields a k-tuple $(a_0, a_1, \ldots, a_{k-1})$. We re-write (6) as

$$m(m - d) \cdots (m - (k - 1)d) = by^2, \; m = n + (k - 1)d. \tag{8}$$

The equation (8) is called the mirror image of (6). The corresponding k-tuple $(a_{k-1}, a_{k-2}, \ldots, a_0)$ is called the mirror image of $(a_0, a_1, \ldots, a_{k-1})$.

Let $P(b) < k$. In Chapter 10 (see Section 10.1), we prove the following result.

Theorem 7. (Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**])

Equation (6) *with* $P(b) < k$ *and* $5 \leq k \leq 100$ *implies that* $(a_0, a_1, \dots, a_{k-1})$ *is among the following tuples or their mirror images.*

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

Theorem 7 with $k = 5$ is due to Mukhopadhyay and Shorey [**45**]. A proof is given in Section 10.2. Theorem 7 with $k = 6$ is due to Bennett, Bruin, Győry and Hajdu [**1**]. They also showed, independently, that (6) with $7 \leq k \leq 11$ and $P(b) \leq 5$ is not possible.

Let $P(b) = k$. Then the case $k = 5$ and $P(b) = k$ in (6) is open. For $k \geq 7$, we prove the following result in Chapter 10 (see Section 10.1).

Theorem 8. (Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**])

Equation (6) *with* $P(b) = k$ *and* $7 \leq k \leq 100$ *implies that* $(a_0, a_1, \dots, a_{k-1})$ *is among the following tuples or their mirror images.*

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

Now we turn to (6) with k as a variable. When d is fixed, Marszalek [**40**] confirmed Conjecture 2 by showing that k is bounded by an explicit constant depending only on d. This was refined by Shorey and Tijdeman [**76**] when $\omega(d)$ is fixed. They showed that (6) implies that k is bounded by a computable number depending only on $\omega(d)$ confirming Conjecture 2 when $\omega(d)$ is fixed. In fact they showed that (6) implies

$$2^{\omega(d)} > c_1 \frac{k}{\log k}$$

which gives

$$d > k^{c_2 \log\log k} \tag{11}$$

where $c_1 > 0$ and $c_2 > 0$ are absolute constants. Laishram [**26**] gave an explicit version of this result by showing

$$k < \begin{cases} 2.25\omega(d)4^{\omega(d)} & \text{if } d \text{ is even}\\ 11\omega(d)4^{\omega(d)} & \text{if } d \text{ is odd}\end{cases}$$

for $\omega(d) \geq 12$ whenever (6) holds. Further Laishram and Shorey [**33**] improved it to

Theorem 9. (Laishram and Shorey [**33**])

Equation (6) *implies that*

$$k < 2\omega(d)2^{\omega(d)}.$$

A proof of Theorem 9 is given in Section 11.5.

Let d be fixed. We consider Conjecture 1. Saradha and Shorey [**63**] solved (6) completely for $d \leq 104$ and $k \geq 4$, see Section 2.4 for earlier results. The following result confirms Conjecture 1 for $d \leq 10^{10}, k \geq 6$ and sharpens (11).

Theorem 10. (Laishram and Shorey [**33**])

Equation (6) *with* $k \geq 6$ *implies that*

$$d > \max(10^{10}, k^{\log\log k}).$$

We give a proof of this theorem in Section 11.6.

Now we turn to Conjecture 1 with $\omega(d)$ fixed. Let $b = 1$. Saradha and Shorey [**63**] proved that (6) with $\omega(d) = 1$ does not hold. In fact they proved it without the condition $\gcd(n, d) = 1$. Thus a product of four or more terms in an arithmetic progression with common difference a prime power can never be a square. We extend this to $\omega(d) = 2$ in the following result.

Theorem 11. (Laishram and Shorey [**33**])

A product of eight or more terms in arithmetic progression with common difference d *satisfying* $\omega(d) = 2$ *is never a square.*

A proof of Theorem 11 is given in Section 11.7. Further we solve (6) with $\omega(d) \leq 5$ and $b = 1$ completely. We have

Theorem 12. (Laishram and Shorey [**33**])

Equation (6) *with* $b = 1$ *and* $\omega(d) \leq 5$ *does not hold.*

A proof of this result is given in Section 10.3. It contains the case $\omega(d) = 1$ already proved by Saradha and Shorey [**63**].

Let $P(b) \leq k$. As stated earlier, equation (6) with $k = 6$ is not possible by Bennett, Bruin, Győry and Hajdu [**1**]. Also (6) with $P(b) < k$ does not hold by Mukhopadhyay and Shorey [**45**] for $k = 5$ and Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**] for $k = 7$. We have no results on (6) with $k \in \{5, 7\}$ and $P(b) = k$. Therefore we assume $k \geq 8$ in the next result. Let $\mathfrak{S}_1$ be the set of tuples $(a_0, \ldots, a_{k-1})$ given by

$$\begin{aligned}
k = 8 &: (2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10);\\
k = 9 &: (2,3,1,5,6,7,2,1,10);\\
k = 13 &: (3,1,5,6,7,2,1,10,11,3,13,14,15), (1,5,6,7,2,1,10,11,3,13,14,15,1)
\end{aligned}$$

and their mirror images. Further $\mathfrak{S}_2$ be the set of tuples $(a_0, a_1, \ldots, a_{k-1})$ given by

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

and their mirror images. We have

Theorem 13. (Laishram and Shorey [**33**])

(*a*) *Equation* (6) *with* $k \geq 8$ *and* $\omega(d) \leq 4$ *implies that either* $\omega(d) = 2, k = 8$, $(a_0, a_1, \ldots, a_7) \in \{(3,1,5,6,7,2,1,10), (10,1,2,7,6,5,1,3)\}$ *or* $\omega(d) = 3$, $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}_1$ *is given by an explicit set of tuples or* $\omega(d) = 4$, $(a_0, a_1, \ldots, a_{k-1}) \in \mathfrak{S}_1 \cup \mathfrak{S}_2$.

(*b*) *Equation* (6) *with* $\omega(d) \in \{5, 6\}$ *and* d *even does not hold.*

A proof of Theorem 13 is given in Section 11.4.

We now consider an equation more general than (6) when $\omega(d) = 1$. Let $k \geq 5, t \geq k - 2$ and $\gamma_1 < \gamma_2 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Thus $t \in \{k, k-1, k-2\}, \gamma_t \geq k - 3$ and $\gamma_i = i - 1$ for $1 \leq i \leq t$ if $t = k$. We put $\psi = k - t$. Let b be a positive squarefree integer and we shall always assume, unless otherwise specified, that $P(b) \leq k$. We consider the equation

$$(n + \gamma_1 d) \cdots (n + \gamma_t d) = by^2 \tag{12}$$

in positive integers n, d, k, b, y, t where n and d are not necessarily relatively prime. Thus n and d need not be relatively prime in Theorem 14 but we always assume that $d \nmid n$ otherwise (12) has infinitely many solutions. When $\psi = 0$, then (12) is the same as (6). Therefore we consider $\psi = 1, 2$.

Let $\psi = 1$. We may assume that $\gamma_1 = 0$ and $\gamma_t = k - 1$ otherwise this is the case $\psi = 0$. It has been shown in [**61**] that

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

are the only squares that are products of $k-1$ distinct integers out of k consecutive integers confirming a conjecture of Erdős and Selfridge [**13**]. This corresponds to the case $b = 1$ and $d = 1$ in (12). In general, it has been proved in [**61**] that (12) with $d = 1$ and $k \geq 4$ implies that $(b, k, n) = (2, 4, 24)$ under the necessary assumption that the left hand side of (12) is divisible by a prime $> k$. Further it has been shown in [**63**, Theorem 4] and [**46**] that (6) with $d > 1$, $\gcd(n, d) = 1, \omega(d) = 1$ and $P(b) < k$ implies that $k \leq 8$.

Let $\psi = 2$. Let $d = 1$. Then it has been shown by Mukhopadhyay and Shorey [**47**, Corollary 3] that a product of $k - 2$ distinct terms out of k consecutive positive integers is a square only if it is given by an explicitly given finite set, see Section 2.6 for a more precise statement. For the general case, it follows from [**47**, Theorem 2] that (12) with $k \geq 6$ is not valid unless $k = 6$ and $n = 45, 240$ whenever the left hand side of (12) is divisible by a prime $> k$. We extend it to $k \geq 5$ in Theorem 2.6.1. In Section 12.4, we prove the following result for $\omega(d) = 1$.

Theorem 14. (Laishram and Shorey [**34**])

Let $\psi = 2, k \geq 15$ and $d \nmid n$. Assume that $P(b) < k$ if $k = 17, 19$. Then (12) *with $\omega(d) = 1$ does not hold.*

As an immediate consequence of Theorem 14, we see that (2.1.1) with $\omega(d) = 1$, $\psi = 0, d \nmid n, k \geq 15$, $P(b) \leq p_{\pi(k)+1}$ if $k = 17, 19$ and $P(b) \leq p_{\pi(k)+2}$ if $k > 19$ does not hold.

CHAPTER 1

A survey of refinements and extensions of Sylvester's theorem

1.1. Sylvester's theorem

Let n, d and $k \geq 2$ be positive integers such that $\gcd(n, d) = 1$. For a pair (n, k) and a positive integer h, we write $[n, k, h]$ for the set of all pairs $(n, k), \cdots, (n + h - 1, k)$ and we set $[n, k] = [n, k, 1] = \{(n, k)\}$.

Let $W(\Delta)$ denote the number of terms in Δ divisible by a prime $> k$. We observe that every prime exceeding k divides at most one term of Δ. On the other hand, a term may be divisible by more than one prime exceeding k. Therefore we have

$$W(\Delta) \leq \omega(\Delta) - \pi_d(k). \tag{1.1.1}$$

If $\max(n, d) \leq k$, we see that $n + (k-1)d \leq k^2$ and therefore no term of Δ is divisible by more than one prime exceeding k. Thus

$$W(\Delta) = \omega(\Delta) - \pi_d(k) \text{ if } \max(n, d) \leq k. \tag{1.1.2}$$

We are interested in finding lower bounds for $P(\Delta)$, $\omega(\Delta)$ and $W(\Delta)$. The first result in this direction is due to Sylvester [**77**] who proved that

$$P(\Delta) > k \text{ if } n \geq d + k. \tag{1.1.3}$$

This immediately gives

$$\omega(\Delta) > \pi_d(k) \text{ if } n \geq d + k. \tag{1.1.4}$$

We give a survey of several results in this direction. The proofs depend on certain estimates from prime number theory stated in Chaper 2.

1.2. Improvements of $\omega(\Delta(n, k)) > \pi(k)$

Let $d = 1$. Let $k = 2$ and $n > 2$. We see that $\omega(n(n+1)) \neq 1$ since $\gcd(n, n+1) = 1$. Thus $\omega(n(n+1)) \geq 2$. Suppose $\omega(n(n+1)) = 2$. Then both n and $n+1$ are prime powers. If either n or $n+1$ is a prime, then $n+1$ or n is a power of 2, respectively. A prime of the form $2^{2^m} + 1$ is called a *Fermat prime* and a prime of the form $2^m - 1$ is called a *Mersenne prime*. Thus we see that either n is a Mersenne prime or $n+1$ is a Fermat prime. Now assume that $n = p^\alpha, n+1 = q^\beta$ where p, q are distinct primes and $\alpha > 1, \beta > 1$. Thus $q^\beta - p^\alpha = 1$ which is Catalan equation. In 1844, Catalan [**2**] conjectured that 8 and 9 are the only perfect powers that differ by 1. Tijdeman [**78**] proved in 1976 that there are only finitely many perfect powers that differ by 1. Catalan's conjecture has been confirmed recently by Mihăilescu [**41**]. Thus $n = 8$ is the only other n for which $\omega(n(n+1)) = 2$. For all other n, we have $\omega(n(n+1)) \geq 3$.

We assume that $k \geq 3$ from now onwards in this section. We observe that

$$\omega(\Delta(n, k)) = \pi(2k) \text{ if } n = k + 1. \tag{1.2.1}$$

If $k+1$ is prime and $2k+1$ is composite, then we observe from (1.2.1) by writing

$$\Delta(k+2, k) = \Delta(k+1, k)\frac{2k+1}{k+1}$$

that

$$\omega(\Delta(k+2,k)) = \pi(2k) - 1. \tag{1.2.2}$$

Let $k+1$ be a prime of the form $3r+2$. Then $2k+1 = 3(2r+1)$ is composite. Since there are infinitely many primes of the form $3r+2$, we see that there are infinitely many k for which $k+1$ is prime and $2k+1$ is composite. Therefore (1.2.2) is valid for infinitely many k. Thus an inequality sharper than $\omega(\Delta(n,k)) \geq \pi(2k) - 1$ for $n > k$ is not valid.

Saradha and Shorey [**61**, Corollary 3] extended the proof of Erdős [**10**] for (1.1.3) to sharpen (1.1.4) and gave explicit bound of $\omega(\Delta(n,k))$ as

$$\omega(\Delta(n,k)) \geq \pi(k) + \left[\frac{1}{3}\pi(k)\right] + 2 \text{ if } n > k \tag{1.2.3}$$

unless $(n,k) \in S_1$ where S_1 is the union of sets

$$\begin{cases} [4,3],[6,3,3],[16,3],[6,4],[6,5,4],[12,5],[14,5,3],[23,5,2], \\ [7,6,2],[15,6],[8,7,3],[12,7],[14,7,2],[24,7],[9,8],[14,8], \\ [14,13,3],[18,13],[20,13,2],[24,13],[15,14],[20,14],[20,17]. \end{cases} \tag{1.2.4}$$

Laishram and Shorey [**28**] improved $\frac{1}{3}$ in (1.2.3) to $\frac{3}{4}$. Define

$$\delta(k) = \begin{cases} 2 & \text{if } \; 3 \leq k \leq 6 \\ 1 & \text{if } \; 7 \leq k \leq 16 \\ 0 & \text{otherwise} \end{cases}$$

so that

$$\left[\frac{3}{4}\pi(k)\right] - 1 + \delta(k) \geq \left[\frac{1}{3}\pi(k)\right] + 2.$$

We have

Theorem 1.2.1. (Laishram and Shorey, [**28**])
Let $n > k$. Then

$$\omega(\Delta(n,k)) \geq \pi(k) + \left[\frac{3}{4}\pi(k)\right] - 1 + \delta(k) \tag{1.2.5}$$

unless

$$(n,k) \in S_1 \cup S_2$$

where S_1 is given by (1.2.4) *and S_2 is the union of sets*

$$\begin{cases} [20,19,3],[24,19],[21,20],[48,47,3],[54,47],[49,48],[74,71,2],[74,72], \\ [74,73,3],[84,73],[75,74],[84,79],[84,83],[90,83],[108,83],[110,83], \\ [90,89],[102,89],[104,89],[108,103],[110,103,2],[114,103,2],[110,104], \\ [114,104],[108,107,12],[109,108,10],[110,109,9],[111,110,7],[112,111,5], \\ [113,112,3],[114,113,7],[138,113],[140,113,2],[115,114,5],[140,114], \\ [116,115,3],[117,116],[174,173],[198,181],[200,181,2],[200,182], \\ [200,193,2],[200,194],[200,197],[200,199,3],[201,200],[282,271,5], \\ [282,272],[284,272,2],[284,273],[278,277,3],[282,277,5],[279,278], \\ [282,278,4],[282,279,3],[282,280],[282,281,7],[283,282,5], \\ [284,283,5],[294,283],[285,284,3],[286,285],[294,293]. \end{cases} \tag{1.2.6}$$

We note here that the right hand sides of (1.2.3) and (1.2.5) are identical for $3 \leq k \leq 18$. Theorem 1.2.1 is an improvement of (1.2.3) for $k \geq 19$. Therefore we shall prove Theorem 1.2.1 for $k \geq 19$. The proof of this theorem uses sharp bounds of π function due to Dusart given by Lemma 3.1.2. We derive the following two results from Theorem 1.2.1. We check that the exceptions in Theorem 1.2.1 satisfy $\omega(\Delta(n,k)) \geq \pi(2k) - 1$. Hence Theorem 1.2.1 gives

COROLLARY 1.2.2. *Let $n > k$. Then*

$$\omega(\Delta(n,k)) \geq \min \left(\pi(k) + \left[\frac{3}{4}\pi(k)\right] - 1 + \delta(k),\ \pi(2k) - 1\right). \tag{1.2.7}$$

Further all the exceptions in Theorem 1.2.1 except $(n,k) \in \{(114,109),(114,113)\}$ satisfy $\omega(\Delta(n,k)) \geq \pi(k) + \left[\frac{2}{3}\pi(k)\right] - 1$. Thus we obtain the following result from Theorem 1.2.1.

COROLLARY 1.2.3. *Let $n > k$. Then*

$$\omega(\Delta(n,k)) \geq \pi(k) + \left[\frac{2}{3}\pi(k)\right] - 1 \tag{1.2.8}$$

unless

$$(n,k) \in \{(114,109),(114,113)\}. \tag{1.2.9}$$

The constant $\frac{3}{4}$ in Theorem 1.2.1 can be replaced by a number close to 1 if $n > \frac{17}{12}k$.

THEOREM 1.2.4. (Laishram and Shorey, [**28**])
Let $(n,k) \neq (6,4)$. Then we have

$$\omega(\Delta(n,k)) \geq \pi(2k) \text{ if } n > \frac{17}{12}k. \tag{1.2.10}$$

The inequality (1.2.10) is an improvement of (1.2.3) for $k \geq 10$. Therefore we shall prove Theorem 1.2.4 for $k \geq 10$. We observe that $\frac{17}{12}k$ in Theorem 1.2.4 is optimal since $\omega(\Delta(34,24)) = \pi(48) - 1$. Also the assumption $(n,k) \neq (6,4)$ is necessary since $\omega(\Delta(6,4)) = \pi(8) - 1$. We recall that there are infinitely many pairs $(n,k) = (k+2,k)$ satisfying (1.2.2). Thus there are infinitely many pairs (n,k) with $n \leq \frac{17}{12}k$ such that $\omega(\Delta(n,k)) < \pi(2k)$. Let $n = k + r$ with $0 < r \leq k$. We observe that every prime p with $k \leq n-1 < p \leq n+k-1$ is a term of $\Delta(n,k)$. Since $k > \frac{n-1}{2}$, we also see that $2p$ is a term in $\Delta(n,k)$ for every prime p with $k < p \leq \frac{n+k-1}{2}$. Further all primes $\leq k$ divide $\Delta(n,k)$. Thus

$$\omega(\Delta(n,k)) = \pi(2k+r-1) - \pi(k+r-1) + \pi(k + \frac{r-1}{2}) = \pi(2k) + F(k,r)$$

where

$$F(k,r) = \pi(2k+r-1) - \pi(2k) - \left(\pi(k+r-1) - \pi(k + \frac{r-1}{2})\right).$$

We use the above formula for finding some pairs (n,k) as given below when $k < 5000$ and $k < n \leq 2k$ for which $\omega(\Delta(n,k)) < \pi(2k)$:

$$\begin{aligned}
\omega(\Delta(n,k)) &= \pi(2k) - 1 \text{ if } (n,k) = (6,4),(34,24),(33,25),(80,57)\\
\omega(\Delta(n,k)) &= \pi(2k) - 2 \text{ if } (n,k) = (74,57),(284,252),(3943,3880)\\
\omega(\Delta(n,k)) &= \pi(2k) - 3 \text{ if } (n,k) = (3936,3879),(3924,3880),(3939,3880)\\
\omega(\Delta(n,k)) &= \pi(2k) - 4 \text{ if } (n,k) = (1304,1239),(1308,1241),(3932,3879)\\
\omega(\Delta(n,k)) &= \pi(2k) - 5 \text{ if } (n,k) = (3932,3880),(3932,3881),(3932,3882).
\end{aligned}$$

It is also possible to replace $\frac{3}{4}$ in Theorem 1.2.1 by a number close to 1 if $n > k$ and k is sufficiently large. Let $k < n < \frac{17}{12}k$. Then

$$\omega(\Delta(n,k)) \geq \pi(n+k-1) - \pi(n-1) + \pi(k).$$

Let $\epsilon > 0$ and $k \geq k_0$ where k_0 exceeds a sufficiently large number depending only on ϵ. Using the estimates (i) and (ii) of Lemma 3.1.2, we get

$$\begin{aligned}\pi(n+k-1)-\pi(n-1) &\geq \frac{n+k-1}{\log(n+k-1)-1}-\frac{n}{\log n}-\frac{1.2762n}{\log^2 n}\\ &\geq \frac{n+k-1}{\log n}-\frac{n}{\log n}-\frac{1.2762n}{\log^2 n}\\ &\geq \frac{k-1}{\log n}-\frac{1.2762k}{\log^2 k}\\ &\geq (1-\epsilon)\pi(k).\end{aligned}$$

Thus $\omega(\Delta(n,k)) \geq (2-\epsilon)\pi(k)$ for $k < n < \frac{17}{12}k$ which we combine with Theorem 1.2.4 to conclude the following result.

Corollary 1.2.5. *Let $\epsilon > 0$ and $n > k$. Then there exists a computable number k_0 depending only on ϵ such that for $k \geq k_0$, we have*

$$\omega(\Delta(n,k)) \geq (2-\epsilon)\pi(k). \tag{1.2.11}$$

Proofs of Theorems 1.2.1 and 1.2.4 are given in *Chapter* 4, see Section 4.1. We end this section with a conjecture of Grimm [**20**]:

Suppose $n, n+1, \cdots, n+k-1$ are all composite numbers, then there are distinct primes p_{i_j} such that $p_{i_j}|(n+j)$ for $0 \leq j < k$.

This conjecture is open. The conjecture implies that if $n, n+1, \cdots, n+k-1$ are all composite, then $\omega(\Delta(n,k)) \geq k$ which is also open. In Chapter 5, we confirm Grimm's Conjecture for $n \leq 1.9 \times 10^{10}$ and for all k. Let $N_0 = 8.5 \times 10^8$. We prove

Theorem 1.2.6. (Laishram and Shorey, [**31**])

Grimm's Conjecture holds for $n \leq p_{N_0}$ and for all k.

We observe that $p_{N_0} = 19236701629 > 1.9 \times 10^{10}$. As a consequence of Theorem 1.2.6, we have

Corollary 1.2.7. *Assume that $n, n+1, \cdots, n+k-1$ are all composite and $n \leq p_{N_0}$. Then*

$$\omega(\Delta(n,k)) \geq k. \tag{1.2.12}$$

Let $g(n)$ be the largest integer such that there exist distinct prime numbers $P_0, \cdots P_{g(n)}$ with $P_i|n+i$. A result of Ramachandra, Shorey and Tijdeman [**52**] states that

$$g(n) > c_1\left(\frac{\log n}{\log\log n}\right)^3$$

where $c_1 > 0$ is a computable absolute constant. Further Ramachandra, Shorey and Tijdeman [**53**] showed that

$$\omega(\Delta(n,k)) \geq k \text{ for } 1 \leq k \leq \exp(c_2(\log n)^{\frac{1}{2}})$$

where c_2 is a computable absolute constant. The proof of these results depend on the theory of linear forms in logarithms. The constants c_1 and c_2 in the above results turns out to be very small. Therefore the above results are valid only for large values of n. Erdős and Selfridge (see [**48**]) showed that Grimm's Conjecture implies that *there is a always a prime between two consecutive squares.* The latter result is out of bounds even after assuming Riemann hypothesis. Thus a proof of Grimm's conjecture is very difficult.

We need to prove only Theorems 1.2.1, 1.2.4 (see Chapter 4) and Theorem 1.2.6 (see Chapter 5) from this section.

1.3. Results on refinement of $P(\Delta(n,k)) > k$

Let $d = 1$. We observe that $P(\Delta(1,k)) \le k$ and therefore, the assumption $n > k$ in (1.1.3) cannot be removed. The assertion (1.1.3) was rediscovered and proved by Schur [**68**] and Erdős [**10**] gave another proof. For $n > k$, Moser [**44**] sharpened (1.1.3) to $P(\Delta(n,k)) > \frac{11}{10}k$ and Hanson [**23**] to $P(\Delta(n,k)) > 1.5k$ unless $(n,k) = (3,2),(8,2),(6,5)$. Further Faulkner [**16**] proved that $P(\Delta(n,k)) > 2k$ if n is greater than or equal to the least prime exceeding $2k$ and $(n,k) \ne (8,2),(8,3)$. We sharpen the results of Hanson and Faulkner. Let $k = 2$. Then we observe (see Lemma 6.1.5) that $P(\Delta(n,k)) > 2k$ unless $n = 3,8$ and that $P(\Delta(3,2)) = P(\Delta(8,2)) = 3$. Thus the estimates (1.3.1)-(1.3.4) are valid for $k = 2$ whenever $n \ne 3,8$ in the case of (1.3.1) and (1.3.2). Therefore we assume $k \ge 3$ from now onwards in this section. Let

$$\begin{aligned}
&E_{10} = \{58\}; \quad E_8 = E_{10} \cup \{59\}; \quad E_6 = E_8 \cup \{60\};\\
&E_4 = E_6 \cup \{12,16,46,61,72,93,103,109,151,163\};\\
&E_2 = E_4 \cup \{4,7,10,13,17,19,25,28,32,38,43,47,62,73,94,104,110,124,152,164,269\}
\end{aligned}$$

and $E_{2i+1} = E_{2i}$ for $1 \le i \le 5$. Further let

$$\begin{aligned}
E_1 = E_2 \cup \{&3,5,6,8,9,11,14,15,18,20,23,26,29,33,35,39,41,44,48,50,53,\\
&56,63,68,74,78,81,86,89,95,105,111,125,146,153,165,173,270\}.
\end{aligned}$$

Finally we denote E_0

$$E_0 = \{(8,3),(6,4),(7,4),(15,13),(16,13)\} \cup \{(k+1,k) : k = 3,4,5,8,11,13,14,18,63\}.$$

Then

Theorem 1.3.1. (Laishram and Shorey, [**30**])

We have

$$P(\Delta(n,k)) > 1.95k \text{ for } n > k \tag{1.3.1}$$

unless $(n,k) \in [k+1,k,h]$ *for* $k \in E_h$ *with* $1 \le h \le 11$ *or* $(n,k) = (8,3)$.

We observe that $P(\Delta(k+1,k)) \le 2k$ and therefore, 1.95 in (1.3.1) cannot be replaced by 2. There are few exceptions if 1.95 is replaced by 1.8 in Theorem 1.3.1. We derive from Theorem 1.3.1 the following result.

Corollary 1.3.2. *We have*

$$P(\Delta(n,k)) > 1.8k \quad \text{for } n > k \tag{1.3.2}$$

unless $(n,k) \in E_0$.

Recently Corollary 1.3.2 has been applied to prove the irreducibility results over rationals for certain Generalised Laguerre polynominals

$$L_m^{(\alpha)}(x) = \sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)}{j!(m-j)!}(-x)^j$$

where $m \in \mathbb{N}$ and $\alpha \in \mathbb{R}$. Schur ([**69**], [**70**]) showed that the polynomials $L_m^{(0)}(x)$, $L_m^{(1)}(x)$ are irreducible for all m. Filaseta, Finch and Leidy [**18**] used Corollary 1.3.2 to give a generalisation of Schur's result. They showed that for all integers $m \ge 1$ and integers α with $0 \le \alpha \le 10$, the polynomial

$$L_m^{(\alpha)}(x) \text{ is irreducible}$$

unless $(m,\alpha) \in \{(2,2),(4,5),(2,7)\}$. We find that for each of these exceptional pairs (m,α), the polynomial $L_m^{(\alpha)}(x)$ has the factor $x-6$ and hence reducible.

The proofs of Theorem 1.3.1 and Corollary 1.3.2 are given in Sections 6.4 and 6.5, respectively.

However if we replace $n > k$ by stronger conditions, then we obtain better estimates of $P(\Delta(n,k))$. In Sections 6.2 and 6.3, we prove the following result.

THEOREM 1.3.3. (Laishram and Shorey, [**30**])

We have

(a)

$$P(\Delta(n,k)) > 2k \text{ for } n > \max(k+13, \frac{279}{262}k). \tag{1.3.3}$$

(b)

$$P(\Delta(n,k)) > 1.97k \text{ for } n > k+13. \tag{1.3.4}$$

We observe that 1.97 in (1.3.4) cannot be replaced by 2 since there are arbitrary long chains of consecutive composite positive integers. The same reason implies that Theorem 1.3.3 **(a)** is not valid under the assumption $n > k+13$. Further the assumption $n > \frac{279}{262}k$ in Theorem 1.3.3 **(a)** is necessary since $P(\Delta(279, 262)) \leq 2 \times 262$.

When k is sufficiently large, we obtain sharper estimates of $P(\Delta(n,k))$. See Shorey and Tijdeman [**73**, Chapter 7]. Ramachandra and Shorey [**51**] proved that

$$P(\Delta(n,k)) > c_4 k \log k \left(\frac{\log\log k}{\log\log\log k}\right)^{\frac{1}{2}} \text{ if } n > k^{\frac{3}{2}}$$

where $c_4 > 0$ is a computable absolute constant. Further it follows from the work of Jutila [**24**] and Shorey [**71**] that

$$P(\Delta(n,k)) > c_5 k \log k \frac{\log\log k}{\log\log\log k} \text{ if } n > k^{\frac{3}{2}}$$

where c_5 is a computable absolute positive constant. If $n \leq k^{\frac{3}{2}}$, it follows from the results on difference between consecutive primes that $\Delta(n,k)$ has a term which is prime. The proof of the result of Ramachandra and Shorey depends on Sieve method and the theory of linear forms in logarithms. The proof of the result of Jutila and Shorey depends on estimates from exponential sums and the theory of linear forms in logarithms. Langevin [**35**], [**36**] proved that for any $\epsilon > 0$,

$$P(\Delta(n,k)) > (1-\epsilon)k \log\log k \text{ if } n \geq c_6 = c_6(k,\epsilon)$$

where c_6 is a computable number depending only on k and ϵ. For an account of results in this direction, see Shorey and Tijdeman [**73**, p. 135].

1.4. Sharpenings of $\omega(\Delta(n,d,k)) \geq \pi_d(k)$ when $d > 1$

Let $d > 1$. The case $k = 2$ is trivial and we assume $k \geq 3$ in this section. We state Schinzel's Hypothesis H [**66**]:

Let $f_1(x), \cdots, f_r(x)$ be irreducible non constant polynomials with integer coefficients and the leading coefficients positive. Assume that for every prime p, there is an integer a such that the product $f_1(a) \cdots f_r(a)$ is not divisible by p. Then there are infinitely many positive integers m such that $f_1(m), \cdots, f_r(m)$ are all primes.

We assume Schinzel's hypothesis. Then $1+d$ and $1+2d$ are primes for infinitely many d. Therefore

$$\omega(\Delta) = \pi(k), \quad k = 3 \tag{1.4.1}$$

for infinitely many pairs $(n,d) = (1,d)$. Let $f_r(x) = 1 + rx$ for $r = 1,2,3,4$. For a given p, we see that $p \nmid f_1(p)f_2(p)\cdots f_4(p)$. Hence there are infinitely many d such that $1+d, 1+2d, 1+3d, 1+4d$ are all primes. Thus

$$\omega(\Delta) = \pi(k) + 1, \ k = 4,5 \tag{1.4.2}$$

for infinitely many pairs $(n,d) = (1,d)$.

Shorey and Tijdeman [**74**] proved that

$$\omega(\Delta) \geq \pi(k). \tag{1.4.3}$$

Thus (1.4.3) is likely to be best possible when $k = 3$ by (1.4.1). In fact, (1.4.3) is likely to be best possible for $k = 3$ when $n = 1$. Moree [**43**] sharpened (1.4.3) to

$$\omega(\Delta) > \pi(k) \text{ if } k \geq 4 \text{ and } (n,d,k) \neq (1,2,5). \tag{1.4.4}$$

If $k = 4, 5$, then (1.4.4) is likely to be best possible by (1.4.2) when $n = 1$.

Saradha and Shorey [**62**] showed that for $k \geq 4$, Δ is divisible by at least 2 distinct primes exceeding k except when $(n,d,k) \in \{(1,5,4),(2,7,4),(3,5,4),\ (1,2,5),(2,7,5),(4,7,5),\ (4,23,5)\}$. Further Saradha, Shorey and Tijdeman [**65**, Theorem 1] improved (1.4.4) to

$$\omega(\Delta) > \frac{6}{5}\pi(k) + 1 \text{ for } k \geq 6 \tag{1.4.5}$$

unless $(n,d,k) \in V_0$ where V_0 is

$$\begin{aligned}&\{(1,2,6),(1,3,6),(1,2,7),(1,3,7),(1,4,7),(2,3,7),(2,5,7),(3,2,7),\\ &(1,2,8),(1,2,11),(1,3,11),(1,2,13),(3,2,13),(1,2,14)\}.\end{aligned} \tag{1.4.6}$$

In fact they derived (1.4.5) from

$$W(\Delta) > \frac{6}{5}\pi(k) - \pi_d(k) + 1 \text{ for } k \geq 6 \tag{1.4.7}$$

unless $(n,d,k) \in V_0$. It is easy to see that the preceding result is equivalent to [**65**, Theorem 2]. By Schinzel's Hypothesis, we observe that (1.4.5) is likely to be best possible for $k = 6, 7$ when $n = 1$. For $k = 8$, we sharpen (1.4.7) by showing

$$W(\Delta) \geq k - 1 - \pi_d(k) \tag{1.4.8}$$

except when

$$\begin{aligned}&n = 1,\ d \in \{2,3,4,5,7\};\\ &n = 2,\ d \in \{3,5\};\ n = 3,\ d = 2;\\ &n = 4,\ d = 3;\ n = 7,\ d \in \{3,5\}.\end{aligned} \tag{1.4.9}$$

Again by Schinzel's Hypothesis, (1.4.8) is likely to be best possible for $k = 8$ when $n = 1$. A proof of (1.4.8) is given in *Section* 7.5.

For $k \geq 9$, Laishram and Shorey [**29**] sharpened (1.4.7) as

THEOREM 1.4.1. (Laishram and Shorey, [**29**])

Let $k \geq 9$ and $(n,d,k) \notin V$ where V is given by

$$\begin{cases} n = 1,\ d = 3,\ k = 9,10,11,12,19,22,24,31;\\ n = 2,\ d = 3,\ k = 12;\ n = 4,\ d = 3,\ k = 9,10;\\ n = 2,\ d = 5,\ k = 9,10;\ n = 1,\ d = 7,\ k = 10.\end{cases} \tag{1.4.10}$$

Then

$$W(\Delta) \geq \pi(2k) - \pi_d(k) - \rho \tag{1.4.11}$$

where

$$\rho = \rho(d) = \begin{cases} 1 \text{ if } d = 2, n \leq k\\ 0 \text{ otherwise}.\end{cases}.$$

When $d = 2$ and $n = 1$, we see that

$$\omega(\Delta) = \pi(2k) - 1$$

and

$$W(\Delta) = \pi(2k) - \pi_d(k) - 1$$

by (1.1.2), for every $k \geq 2$. This is also true for $n = 3, d = 2$ and $2k+1$ is not a prime. Thus (1.4.11) is best possible when $d = 2$. We see from Theorem 1.4.1 and (1.1.1) that

$$\omega(\Delta) \geq \pi(2k) - \rho \text{ if } (n,d,k) \notin V. \tag{1.4.12}$$

For $(n, d, k) \in V$, we see that $\omega(\Delta) = \pi(2k) - 1$ except at $(n, d, k) = (1, 3, 10)$. This is also the case for $(n, d, k) \in V_0$ with $k = 6, 7, 8$. Now, we apply Theorem 1.4.1, (1.4.5) for $k = 6, 7, 8$ and (1.4.4) for $k = 4, 5$ to get the following result immediately.

Corollary 1.4.2. *Let $k \geq 4$. Then*

$$\omega(\Delta) \geq \pi(2k) - 1 \tag{1.4.13}$$

except at $(n, d, k) = (1, 3, 10)$.

This solves a conjecture of Moree [**43**]. The proof of Theorem 1.4.1 is given in *Section* 7.4.

1.5. Results on refinements of $P(\Delta(n, d, k)) > k$ for $d > 1$

We observe that $P(\Delta(n, d, 2)) = 2$ if and only if $n = 1, d = 2^r - 1$ with $r > 1$. Therefore we suppose that $k \geq 3$ in this section. Let $d = 2$. If $n > k$, then (1.5.2) follows from Theorem 1.4.1. Let $n \leq k$. Then we observe that $P(\Delta(n, 2, k)) \leq 2k$ implies $P(\Delta(n + k, 1, k)) \leq 2k$. Therefore the case $d = 2$ when considering $P(\Delta(n, 2, k)) > 2k$ reduces to considering $P(\Delta(n + k, 1, k)) > 2k$ discussed above in the case $d = 1$. Therefore we may suppose that $d > 2$.

Langevin [**38**] sharpened (1.1.3) to

$$P(\Delta) > k \text{ if } n > k.$$

Shorey and Tijdeman [**75**] improved the above result as

$$P(\Delta) > k \quad \text{unless} \quad (n, d, k) = (2, 7, 3). \tag{1.5.1}$$

We have

Theorem 1.5.1. (Laishram and Shorey, [**32**])

Let $d > 2$. Then

$$P(\Delta) > 2k \tag{1.5.2}$$

unless (n, d, k) is given by

$$\begin{aligned} k = 3,\ & n = 1, d = 4, 7;\\ & n = 2, d = 3, 7, 23, 79;\\ & n = 3, d = 61;\ n = 4, d = 23;\\ & n = 5, d = 11;\ n = 18, d = 7;\\ k = 4,\ & n = 1, d = 3, 13;\ n = 3, d = 11;\\ k = 10,\ & n = 1, d = 3. \end{aligned}$$

It is necessary to exclude the exceptions stated in Theorem 1.5.1. A proof of Theorem 1.5.1 is given in Chapter 8. It depends on Theorem 1.4.1 and the theory of linear forms in logarithms.

CHAPTER 2

A survey of results on squares in products of terms in an arithmetic progression

2.1. Introduction

Let n, d, k, b, y be positive integers such that b is square free, $d \geq 1$, $k \geq 2$, $P(b) \leq k$ and $\gcd(n, d) = 1$. We consider the equation

$$\Delta(n, d, k) = n(n+d) \cdots (n+(k-1)d) = by^2. \tag{2.1.1}$$

If $k = 2$, we observe that (2.1.1) has infinitely many solutions. Therefore we always suppose that $k \geq 3$. Let $p > k, p|(n+id)$. Then $p \nmid (n+jd)$ for $j \neq i$ otherwise $p|(i-j)$ and $|i-j| < k$. Equating powers of p on both sides of (2.1.1), we see that $\mathrm{ord}_p(n+id)$ is even. From (2.1.1), we have

$$n + id = a_i x_i^2 = A_i X_i^2 \tag{2.1.2}$$

with a_i squarefree and $P(a_i) \leq k$, $P(A_i) \leq k$ and $(X_i, \prod_{p<k} p) = 1$ for $0 \leq i < k$. Since $\gcd(n, d) = 1$, we also have

$$(A_i, d) = (a_i, d) = (X_i, d) = (x_i, d) = 1 \quad \text{for } 0 \leq i < k. \tag{2.1.3}$$

We call $(a_{k-1}, a_{k-2}, \cdots, a_1, a_0)$ as the mirror image of $(a_0, a_1, a_2, \cdots, a_{k-1})$.

Let $d = 1$. We recall that $\Delta(n, 1, k) = \Delta(n, k)$. Several particular cases of (2.1.1) have been treated by many mathematicians. We refer to Dickson [**5**] for a history. It is a consequence of some old diophantine results that (2.1.1) with $k = 3$ is possible only when $n = 1, 2, 48$. Let $k \geq 4$. As mentioned in the beginning of Section 1.2, there are infinitely many pairs (n, k) such that $P(\Delta(n, k)) \leq k$. Then (2.1.1) is satisfied with $P(y) \leq k$ for these infinitely many pairs. Therefore we consider (2.1.1) with $P(\Delta(n, k)) > k$. This assumption is satisfied when $n > k$ by (1.1.3). Developing on the earlier work of Erdős [**11**] and Rigge [**55**], it was shown by Erdős and Selfridge [**13**] that (2.1.1) with $n > k^2$ and $P(b) < k$ does not hold. Suppose $P := P(\Delta(n, k)) > k$. Then there is a unique i with $0 \leq i < k$ such that $n+i$ is divisible by P. Hence by (2.1.1), $n+i$ is divisible by P^2 showing that $n + i \geq (k+1)^2$ giving $n > k^2$. Thus it follows from the result of Erdős and Selfridge [**13**] that (2.1.1) with $P > k$ and $P(b) < k$ does not hold. The assumption $P(b) < k$ has been relaxed to $P(b) \leq k$ in Saradha [**60**].

Therefore we suppose that $d > 1$. Let $k = 3$. Then it follows from infinitude of solutions of Pell's equation that there are infinitely many solutions of (2.1.1). Therefore we assume from now onward that $k \geq 4$. Fermat (see Mordell [**42**, p.21]) showed that there are no four squares in an arithmetic progression. Euler proved a more general result that a product of four terms in arithmetic progression can never be a square. We prove the following result in Section 10.9.

Theorem 2.1.1. (Hirata-Kohno, Laishram, Shorey and Tijdeman, [**25**]) *Equation* (2.1.1) *with* $4 \leq k \leq 109$ *and* $b = 1$ *is not possible.*

By Euler, Theorem 2.1.1 is valid when $k = 4$. The case when $k = 5$ is due to Obláth [**50**]. Independently, Bennett, Bruin, Győry and Hajdu [**1**] proved that (2.1.1) with $6 \leq k \leq 11$ does not hold.

We know that (2.1.1) with $k = 4$ and $b = 6$ has infinitely many solutions. A general conjecture states that Δ is divisible by a prime $> k$ to an odd power. In other words,

Conjecture 2.1.2. *Equation* (2.1.1) *with* $P(b) \leq k$ *implies that* $k = 4, b = 6$.

A weaker version of Conjecture 2.1.2 is the following conjecture due to Erdős.

CONJECTURE 2.1.3. *Equation* (2.1.1) *with* $P(b) \leq k$ *implies* k *is bounded by a computable absolute constant.*

Granville (unpublished) showed that Conjecture 2.1.3 follows from Oesterlé and Masser's *abc*-conjecture, see Laishram [**27**, Section 9.4] for a proof. Now we turn to results towards Conjectures 2.1.2 and 2.1.3.

2.2. Conjecture 2.1.2 with k fixed

Let k be fixed. As already stated, (2.1.1) with $k = 4$ and $b = 6$ has infinitely many solutions. On the other hand, (2.1.1) with $k = 4$ and $b \neq 6$ does not hold. Therefore we consider (2.1.1) with $k \geq 5$. By (2.1.2), the equation (2.1.1) yields a k-tuple $(a_0, a_1, \ldots, a_{k-1})$. We re-write (2.1.1) as

$$m(m-d)\cdots(m-(k-1)d) = by^2, \ m = n+(k-1)d. \tag{2.2.1}$$

The equation (2.2.1) is called the mirror image of (2.1.1). The corresponding k-tuple $(a_{k-1}, a_{k-2}, \ldots, a_0)$ is called the mirror image of $(a_0, a_1, \ldots, a_{k-1})$.

Let $P(b) < k$. In Chapter 10 (see Section 10.1), we prove the following result.

THEOREM 2.2.1. (Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**]) *Equation* (2.1.1) *with* $P(b) < k$ *and* $5 \leq k \leq 100$ *implies that* $(a_0, a_1, \ldots, a_{k-1})$ *is among the following tuples or their mirror images.*

$$\begin{aligned} k = 8 &: (2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10);\\ k = 9 &: (2,3,1,5,6,7,2,1,10);\\ k = 14 &: (3,1,5,6,7,2,1,10,11,3,13,14,15,1);\\ k = 24 &: (5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3,7). \end{aligned} \tag{2.2.2}$$

Theorem 2.2.1 with $k = 5$ is due to Mukhopadhyay and Shorey [**45**]. A different proof is given in Section 10.2. Initially, Bennett, Bruin, Győry, Hajdu [**1**] and Hirata-Kohno, Shorey (unpublished), independently, proved Theorem 2.2.1 with $k = 6$ and $(a_0, a_1, \ldots .a_5) \neq (1,2,3,1,5,6), (6,5,1,3,2,1)$. Next Bennett, Bruin, Győry and Hajdu [**1**] removed the assumption on $(a_0, a_1, \ldots, a_5)$ in the above result. They also showed, independently, that (2.1.1) with $7 \leq k \leq 11$ and $P(b) \leq 5$ is not possible. This is now a special case of Theorem 2.2.1.

Let $P(b) = k$. The case $k = 5$ and $P(b) = 5$ in (2.1.1) is still open. For $k \geq 7$, Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**] showed that

THEOREM 2.2.2. (Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**]) *Equation* (2.1.1) *with* $P(b) = k$ *and* $7 \leq k \leq 100$ *implies that* $(a_0, a_1, \cdots, a_{k-1})$ *is among the following tuples or their mirror images.*

$$\begin{aligned} k = 7 &: (2,3,1,5,6,7,2), (3,1,5,6,7,2,1), (1,5,6,7,2,1,10);\\ k = 13 &: (3,1,5,6,7,2,1,10,11,3,13,14,15),\\ &\quad\ (1,5,6,7,2,1,10,11,3,13,14,15,1);\\ k = 19 &: (1,5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22);\\ k = 23 &: (5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3),\\ &\quad\ (6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3,7). \end{aligned} \tag{2.2.3}$$

A proof of Theorem 2.2.2 is given in Chapter 10 (see Section 10.1).

2.3. Equation (2.1.1) with k as a variable

Let us now consider (2.1.1) with k as a variable. When d is fixed, Marszalek [**40**] confirmed Conjecture (2.1.3) by showing that k is bounded by a computable constant depending only on d. This was refined by Shorey and Tijdeman [**76**] when $\omega(d)$ is fixed. They showed that (2.1.1) implies that k is bounded by a computable number depending only on $\omega(d)$ confirming Conjecture (2.1.3) when $\omega(d)$ is fixed. In fact they showed that (2.1.1) implies

$$2^{\omega(d)} > c_1 \frac{k}{\log k} \tag{2.3.1}$$

which gives

$$d > k^{c_2 \log\log k} \tag{2.3.2}$$

where $c_1 > 0$ and $c_2 > 0$ are absolute constants. Laishram [**26**] gave an explicit version of (2.3.1) by showing

$$k < \begin{cases} 2.25\omega(d)4^{\omega(d)} & \text{if } d \text{ is even} \\ 11\omega(d)4^{\omega(d)} & \text{if } d \text{ is odd} \end{cases}$$

for $\omega(d) \geq 12$ whenever (2.1.1) holds. Further Laishram and Shorey [**33**] improved it to

Theorem 2.3.1. (Laishram and Shorey [**33**])
Equation (2.1.1) *implies that*

$$k < 2\omega(d)2^{\omega(d)}.$$

A proof of Theorem 2.3.1 is given in Section 11.5.

2.4. Conjecture 2.1.2 with d fixed

Let d be fixed. We consider Conjecture 2.1.2. For a given value of d, we observe that (2.1.1) with $k \in \{4, 5\}$ can be solved via finding all the integral points on elliptic curves by MAGMA or SIMATH as in [**17**] and [**63**]. Equation (2.1.1) was completely solved for $k \geq 4$ and $1 < d \leq 104$ in Saradha and Shorey [**63**]. For earlier results, see Saradha [**59**] and Filakovszky and Hajdu [**17**]. The following theorem confirms Conjecture 2.1.2 for $d \leq 10^{10}$ and $k \geq 6$.

Theorem 2.4.1. (Laishram and Shorey [**33**])
Equation (2.1.1) *with* $k \geq 6$ *implies that*

$$d > \max(10^{10}, k^{\log\log k}).$$

We give a proof of this theorem in Section 11.6.

2.5. Equation (2.1.1) with $\omega(d)$ fixed

Let $\omega(d)$ be fixed. Let $b = 1$. Saradha and Shorey [**63**] proved that (2.1.1) with $\omega(d) = 1$ does not hold. In fact they proved it without the condition $\gcd(n, d) = 1$. Thus a product of four or more terms in an arithmetic progression with common difference a prime power can never be a square. We extend this to $\omega(d) = 2$ in the following result.

Theorem 2.5.1. (Laishram and Shorey [**33**])
A product of eight or more terms in arithmetic progression with common difference d satisfying $\omega(d) = 2$ is never a square.

A proof of Theorem 2.5.1 is given in Section 11.7. However we solve (2.1.1) with $\omega(d) \leq 5$ and $b = 1$ completely when $\gcd(n, d) = 1$. We have

Theorem 2.5.2. (Laishram and Shorey [**33**])
Equation (2.1.1) *with* $b = 1$ *and* $\omega(d) \leq 5$ *does not hold.*

A proof of this result is given in Section 11.3. Theorem 2.5.2 contains the case $\omega(d) = 1$ already proved by Saradha and Shorey [**63**].

Let $P(b) \leq k$. As stated earlier, equation (2.1.1) with $k = 6$ is not possible by Bennett, Bruin, Győry and Hajdu [**1**]. Also (2.1.1) with $P(b) < k$ does not hold by Mukhopadhyay and Shorey [**45**] for $k = 5$ and Hirata-Kohno, Laishram, Shorey and Tijdeman [**25**] for $k = 7$. We have no results on

(2.1.1) with $k \in \{5, 7\}$ and $P(b) = k$. Therefore we assume $k \geq 8$ in the next result. Let $\mathfrak{S}_1$ be the set of tuples $(a_0, \dots, a_{k-1})$ given by

$$\begin{aligned} k = 8 &: (2,3,1,5,6,7,2,1), (3,1,5,6,7,2,1,10);\\ k = 9 &: (2,3,1,5,6,7,2,1,10);\\ k = 13 &: (3,1,5,6,7,2,1,10,11,3,13,14,15), (1,5,6,7,2,1,10,11,3,13,14,15,1)\end{aligned}$$

and their mirror images. Further $\mathfrak{S}_2$ be the set of tuples $(a_0, a_1, \dots, a_{k-1})$ given by

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

and their mirror images. We have

Theorem 2.5.3. (Laishram and Shorey [**33**])
(*a*) *Equation* (2.1.1) *with* $k \geq 8$ *and* $\omega(d) \leq 4$ *implies that either* $\omega(d) = 2, k = 8$, $(a_0, a_1, \dots, a_7) \in \{(3,1,5,6,7,2,1,10), (10,1,2,7,6,5,1,3)\}$ *or* $\omega(d) = 3$, $(a_0, a_1, \dots, a_{k-1}) \in \mathfrak{S}_1$ *or* $\omega(d) = 4$, $(a_0, a_1, \dots, a_{k-1}) \in \mathfrak{S}_1 \cup \mathfrak{S}_2$.
(*b*) *Equation* (2.1.1) *with* $\omega(d) \in \{5, 6\}$ *and* d *even does not hold.*

A proof of Theorem 2.5.3 is given in Section 11.4. Theorem 2.5.3 contains already proved case $\omega(d) = 1$ where it has been shown in [**63**] for $k > 29$ and [**45**] for $4 \leq k \leq 29$ that (2.1.1) implies that either $k = 4, (n, d, b, y) = (75, 23, 6, 140)$ or $k = 5, P(b) = k$. We do not use this result in the proof of Theorem 2.5.3.

2.6. Equation $\Delta(n, d, k) = by^2$ with $\omega(d) = 1$ and at most two terms omitted

We now consider a equation more general than (6). Let $k \geq 5, t \geq k - 2$ and $\gamma_1 < \gamma_2 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Thus $t \in \{k, k-1, k-2\}, \gamma_t \geq k - 3$ and $\gamma_i = i - 1$ for $1 \leq i \leq t$ if $t = k$. We put $\psi = k - t$. Let b be a positive squarefree integer and we shall always assume, unless otherwise specified, that $P(b) \leq k$. We consider the equation

$$(n + \gamma_1 d) \cdots (n + \gamma_t d) = by^2 \tag{2.6.1}$$

in positive integers n, d, k, b, y, t. We shall follow the above assumptions stated in this section whenever we refer to (2.6.1). When $\psi = 0$, then (2.6.1) is the same as (2.1.1). Therefore we consider $\psi = 1, 2$.

Let $\psi = 1$. We may assume that $\gamma_1 = 0$ and $\gamma_t = k - 1$ otherwise this is the case $\psi = 0$. It has been shown in [**61**] that

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

are the only squares that are products of $k-1$ distinct integers out of k consecutive integers confirming a conjecture of Erdős and Selfridge [**13**]. This corresponds to the case $b = 1$ and $d = 1$ in (2.6.1). In general, it has been proved in [**61**] that (2.6.1) with $d = 1$ and $k \geq 4$ implies that $(b, k, n) = (2, 4, 24)$ under the necessary assumption that the left hand side of (2.6.1) is divisible by a prime $> k$. Further it has been shown in [**63**, Theorem 4] and [**46**] that (2.1.1) with $d > 1$, $\gcd(n, d) = 1, \omega(d) = 1$ and $P(b) < k$ implies that $k \leq 8$.

Let $\psi = 2$. Let $d = 1$. Then it has been shown in [**47**, Corollary 3] that a product of $k - 2$ distinct terms out of k consecutive positive integers is a square only if it is given by

$$\frac{6!}{1.5} = \frac{7!}{5.7} = 12^2, \ \frac{10!}{1.7} = \frac{11!}{7.11} = 720^2.$$

and

$$\begin{cases} \frac{4!}{2.3} = 2^2, \ \frac{6!}{4.5} = 6^2, \ \frac{8!}{2.5.7} = 24^2, \ \frac{10!}{2.3.4.6.7} = 60^2, \ \frac{9!}{2.5.7} = 72^2, \\ \frac{10!}{2.3.6.7} = 120^2, \ \frac{10!}{2.7.8} = 180^2, \ \frac{10!}{7.9} = 240^2, \ \frac{10!}{4.7} = 360^2, \\ \frac{21!}{13!.17.19} = 5040^2, \ \frac{14!}{2.3.4.11.13} = 5040^2, \ \frac{14!}{2.3.11.13} = 10080^2. \end{cases}$$

These corresponds to (2.1.1) with $b = 1$. For the general case, we have

Theorem 2.6.1.
Let $\psi = 2, d = 1$ and $k \geq 5$. Assume that the left hand side of (2.6.1) *is divisible by a prime $> k$. Then* (2.6.1) *is not valid unless $k = 5, n \in \{45, 46, 47, 48, 96, 239, 240, 241, 242, 359, 360\}$ and $k = 6$, $n \in \{45, 240\}$.*

We observe that $n + k - 1 \geq p^2_{\pi(k)+1} \geq (k+1)^2$ since the left hand side of (2.6.1) is divisible by a prime $> k$. Thus $n > k^2$ and the assertion for $k \geq 6$ follows immediately from [**47**, Theorem 2]. Let $k = 5$. Then $n \geq 7^2 - 4 = 45$. Multiplying both sides of (2.1.1) by b^3 and putting $X = b(n + \gamma_2), Y = b^2 y$, we get the elliptic curve

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

For each choice of triplets $(\gamma_1, \gamma_2, \gamma_3)$ with $0 \leq \gamma_1 < \gamma_2 < \gamma_3 \leq 4$ and for each $b \in \{1, 2, 3, 6, 5, 10, 15, 30\}$, we check for the integral points on the elliptic curve using **MAGMA**. Observing that $b|X, b^2|Y$ and $X = b(n + \gamma_2) \geq 45b$, we find that all the solutions of (2.1.1) are given by those listed in the assertion of Theorem 2.6.1. For instance, when $(\gamma_1, \gamma_2, \gamma_3) = (0, 2, 4)$ and $b = 3$, we have the curve $Y^2 = X^3 - 36X$ and the integral points with $X \geq 45b$ is $X = 294, Y = 5040$. Then $n + 2 = \frac{294}{3} = 98$ giving $n = 96$ and we see that $96 \cdot 98 \cdot 100 = 12(4 \times 7 \times 10)^2$ gives a solution.

Let $d > 1$. In Section 12.4, we prove the following result.

Theorem 2.6.2. (Laishram and Shorey [**34**])
Let $\psi = 2, k \geq 15$. Assume that $P(b) < k$ if $k = 17, 19$. Then (2.6.1) *with $\omega(d) = 1$ does not hold.*

As an immediate consequence of Theorem 2.6.2, we see that (2.1.1) with $\omega(d) = 1$, $\psi = 0, d \nmid n, k \geq 15$, $P(b) \leq p_{\pi(k)+1}$ if $k = 17, 19$ and $P(b) \leq p_{\pi(k)+2}$ if $k > 19$ does not hold. For the proof, we delete the terms, if any, divisibly by primes $\{k, p_{\pi(k)+1}\}$ if $k = 17, 19$ and $\{p_{\pi(k)+1}, p_{\pi(k)+2}\}$ otherwise. Then the assertion follows from Theorem 2.6.2.

The assumption $\gcd(n, d) = 1$ can be replaced by $d \nmid n$ in Theorem 2.6.2. Consider Theorem 2.6.2 with $\gcd(n, d) > 1$. Let $p^\beta =$gcd(n, d), $n' = \frac{n}{p^\beta}$ and $d' = \frac{d}{p^\beta}$. Then $d' > 1$ since $d \nmid n$. Now, by dividing $(p^\beta)^t$ on both sides of (2.6.1), we have

$$(n' + \gamma_1 d') \cdots (n' + \gamma_t d') = p^\epsilon b' y'^2 \tag{2.6.2}$$

where $y' > 0$ is an integer with $P(b') \leq k$, $P(b') < k$ when $k = 17$ and $\epsilon \in \{0, 1\}$. Since $p|d'$ and $\gcd(n', d') = 1$, we see that $p \nmid (n' + \gamma_1 d') \cdots (n' + \gamma_t d')$ giving $\epsilon = 0$ and assertion follows.

CHAPTER 3

Results from prime number theory

In this chapter, we state the results from Prime Number Theory and related areas which we will be using in the proofs in the subsequent chapters.

3.1. Estimates of some functions on primes and Stirling's formula

We begin with the bounds for $\pi(\nu)$ given by Rosser and Schoenfeld, see [**58**, p. 69-71].

LEMMA 3.1.1. *For $\nu > 1$, we have*

(*i*) $\pi(\nu) < \dfrac{\nu}{\log \nu}\left(1 + \dfrac{3}{2\log \nu}\right)$

(*ii*) $\pi(\nu) > \dfrac{\nu}{\log \nu - \frac{1}{2}}$ for $\nu \geq 67$

(*iii*) $\displaystyle\prod_{p^a \leq \nu} p^a < (2.826)^\nu$

(*iv*) $\displaystyle\prod_{p \leq \nu} p < (2.763)^\nu$

(*v*) $p_i \geq i \log i$ for $i \geq 2$.

The following sharper estimates are due to Dusart [**6**, p.14; Prop 1.7]. See also [**7**, p.55], [**8**, p.414].

LEMMA 3.1.2. *For $\nu > 1$, we have*

(*i*) $\pi(\nu) \leq \dfrac{\nu}{\log \nu}\left(1 + \dfrac{1.2762}{\log \nu}\right) =: a(\nu)$

(*ii*) $\pi(\nu) \geq \dfrac{\nu}{\log \nu - 1} =: b(\nu)$ for $\nu \geq 5393$

(*iii*) $\displaystyle\prod_{p \leq \nu} p < 2.71851^\nu$.

The next lemma is on the estimate of $\sum_{p \leq p_i} \log p$ due to G. Robin [**56**, Theorem 6].

LEMMA 3.1.3. *For $i \geq 2$, we have*

$$\sum_{p \leq p_i} \log p > i(\log i + \log\log i - 1.076868).$$

The following lemma is due to Ramaré and Rumely [**54**, Theorems 1, 2].

LEMMA 3.1.4. *Let $k \in \{3, 4, 5, 7\}$, l be a positive integer such that gcd$(l, k) = 1$ and*

$$\theta(x, k, l) = \sum_{\substack{p \leq x \\ p \equiv l (\text{mod } k)}} \log p.$$

Then for $x_0 \leq 10^{10}$, we have

$$\theta(x, k, l) \geq \begin{cases} \frac{x}{\phi(k)}(1 - \epsilon') \text{ for } x \geq 10^{10} \\ \frac{x}{\phi(k)}\left(1 - \frac{\epsilon\phi(k)}{\sqrt{x_0}}\right) \text{ for } 10^{10} > x \geq x_0 \end{cases} \tag{3.1.1}$$

and

$$\theta(x,k,l) \leq \begin{cases} \frac{x}{\phi(k)}(1+\epsilon') \text{ for } x \geq 10^{10} \\ \frac{x}{\phi(k)}\left(1+\frac{\epsilon\phi(k)}{\sqrt{x_0}}\right) \text{ for } 10^{10} > x \geq x_0 \end{cases} \tag{3.1.2}$$

where $\epsilon := \epsilon(k)$ *and* $\epsilon' := \epsilon'(k)$ *are given by*

k	3	4	5	7
ϵ	1.798158	1.780719	1.412480	1.105822
ϵ'	0.002238	0.002238	0.002785	0.003248

In the next lemma, we derive estimates for $\pi(x,k,l)$ and $\pi(2x,k,l)-\pi(x,k,l)$ from Lemma 3.1.4.

LEMMA 3.1.5. *Let* $k \in \{3,4,5,7\}$ *and* l *be a positive integer such that* $gdc(l,k)=1$. *Then we have*

$$\pi(x,k,l) \geq \frac{x}{\log x}\left(\mathfrak{c}_1 + \frac{\mathfrak{c}_2}{\log\frac{x}{2}}\right) \ for\ x \geq x_0 \tag{3.1.3}$$

and

$$\pi(2x,k,l)-\pi(x,k,l) \leq \mathfrak{c}_3\frac{x}{\log x} \ for\ x \geq x_0 \tag{3.1.4}$$

where $\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3$ *and* x_0 *are given by*

k	3	4	5	7
$\mathfrak{c}_1$	0.488627	0.443688	0.22175	0.138114
$\mathfrak{c}_2$	0.167712	0.145687	0.0727974	0.043768
$\mathfrak{c}_3$	0.527456	0.6359475	0.3182006	0.235598
x_0	25000	1000	2500	1500

PROOF. We have

$$\theta(x,k,l) = \sum_{\substack{p\leq x \\ p\equiv l (\text{mod } k)}} \log p \leq \pi(x,k,l)\log x$$

so that

$$\pi(x,k,l) \geq \frac{\theta(x,k,l)}{\log x}. \tag{3.1.5}$$

Also,

$$\theta(x,k,l) \leq \pi(\frac{x}{2},k,l)\log\frac{x}{2} + \left(\pi(x,k,l)-\pi(\frac{x}{2},k,l)\right)\log x = \pi(x,k,l)\log x - \pi(\frac{x}{2},k,l)\log 2$$

giving

$$\pi(x,k,l)\log x \geq \theta(x,k,l) + \pi(\frac{x}{2},k,l)\log 2.$$

Now we use (3.1.5) for $\frac{x}{2}$ to derive

$$\pi(x,k,l) \geq \frac{x}{\log x}\left(\frac{\theta(x,k,l)}{x} + \frac{\theta(\frac{x}{2},k,l)\log 2}{x}\frac{1}{\log\frac{x}{2}}\right). \tag{3.1.6}$$

Let $k=3,4,5,7$ and $x_0 := x_0(k)$ be as given in the statement of the lemma. Since $x_0 \leq 50000 \leq (\frac{\epsilon\phi(k)}{\epsilon'})^2$, we have from (3.1.1) that

$$\begin{aligned} \theta(x,k,l) &\geq \frac{x}{\phi(k)}\left(1-\frac{\epsilon\phi(k)}{\sqrt{x_0}}\right) \text{ for } x \geq x_0, \\ \theta(\frac{x}{2},k,l) &\geq \frac{x}{2\phi(k)}\left(1-\frac{\epsilon\phi(k)}{\sqrt{\frac{x_0}{2}}}\right) \text{ for } x \geq x_0. \end{aligned} \tag{3.1.7}$$

This with (3.1.6) implies (3.1.3). Further we also have from (3.1.2) that

$$\theta(2x,k,l) \leq \frac{2x}{\phi(k)}\left(1+\frac{\epsilon\phi(k)}{\sqrt{2x_0}}\right) \text{ for } x \geq x_0.$$

This with (3.1.7), (3.1.6) and

$$\theta(2x,k,l)-\theta(x,k,l) \geq (\pi(2x,k,l)-\pi(x,k,l))\log x$$

implies

$$\begin{aligned}\pi(2x,k,l)-\pi(x,k,l) \leq & \frac{x}{\log x}\left(\frac{2}{\phi(k)}(1+\frac{\epsilon\phi(k)}{\sqrt{2x_0}}-\frac{1}{\phi(k)}(1-\frac{\epsilon\phi(k)}{\sqrt{x_0}})\right) \\ = & \frac{x}{\log x}\left(\frac{1}{\phi(k)}+\frac{(1+\sqrt{2})\epsilon}{\sqrt{x_0}}\right) \leq \mathfrak{c}_3\frac{x}{\log x}\end{aligned}$$

for $x \geq x_0$, giving (3.1.4). □

The next lemma gives a lower bound for $\mathrm{ord}_p(k-1)!$.

Lemma 3.1.6. *For a prime $p < k$, we have*

$$\mathrm{ord}_p(k-1)! \geq \frac{k-p}{p-1}-\frac{\log(k-1)}{\log\ p}.$$

Proof. Let $p^h \leq k-1 < p^{h+1}$. Then we have

$$\mathrm{ord}_p(k-1)! = \left[\frac{k-1}{p}\right]+\cdots+\left[\frac{k-1}{p^h}\right].$$

Now, we note that $\left[\frac{k-1}{p^i}\right] \geq \frac{k-1}{p^i}-\frac{p^i-1}{p^i} = \frac{k}{p^i}-1$ for $i \geq 1$. Hence

$$\mathrm{ord}_p(k-1)! \geq \sum_{i=1}^{h}\left(\frac{k}{p^i}-1\right) = \frac{k}{p-1}(1-\frac{1}{p^h})-h = \frac{k}{p-1}-\frac{1}{p-1}\frac{k}{p^h}-h.$$

Since $p^h \leq k-1 < k \leq p^{h+1}$, we have $h \leq \frac{\log(k-1)}{\log p}$ and $\frac{k}{p^h} \leq p$, which we use in the estimate for $\mathrm{ord}_p((k-1)!)$ above to get the lemma. □

We end this chapter with a lemma on Stirling's formula, see Robbins [**57**].

Lemma 3.1.7. *For a positive integer ν, we have*

$$\sqrt{2\pi\nu}\ e^{-\nu}\nu^{\nu}e^{\frac{1}{12\nu+1}} < \nu! < \sqrt{2\pi\nu}\ e^{-\nu}\nu^{\nu}e^{\frac{1}{12\nu}}.$$

Part 1

Proof of results on refinements and extensions of Sylvester's theorem

CHAPTER 4

Refinement of Sylvester's theorem on the number of prime divisors in a product of consecutive integers: Proof of Theorems 1.2.1 and 1.2.4

In this chapter we prove Theorems 1.2.1 and 1.2.4. For $x \geq k$, we write

$$\Delta' = \Delta'(x, k) = \Delta(x - k + 1, k).$$

4.1. An Alternative Formulation

As remarked in Section 1.2, we prove Theorem 1.2.1 for $k \geq 19$ and Theorem 1.2.4 for $k \geq 10$. Further we derive these two theorems from the following more general result.

THEOREM 4.1.1.

(a) *Let $k \geq 19$, $x \geq 2k$ and $(x, k) \notin S_3$ where S_3 is the union of all sets $[x, k, h]$ such that $[x - k + 1, k, h]$ belongs to S_2 given by* (1.2.6). *Let $f_1 < f_2 < \cdots < f_\mu$ be all the integers in $[0, k)$ satisfying*

$$P((x - f_1) \cdots (x - f_\mu)) \leq k. \tag{4.1.1}$$

Then

$$\mu \leq k - \left[\frac{3}{4}\pi(k)\right] + 1. \tag{4.1.2}$$

(b) *Let $k \geq 10$, $x > \frac{29}{12}k - 1$. Assume* (4.1.1). *Then we have*

$$\mu \leq k - M(k) \tag{4.1.3}$$

where

$$M(k) = \max(\pi(2k) - \pi(k), \left[\frac{3}{4}\pi(k)\right] - 1). \tag{4.1.4}$$

Thus, under the assumptions of the theorem, we see that the number of terms in $\Delta' = x(x - 1) \cdots (x - k + 1)$ divisible by a prime $> k$ is at least $k - \mu$. Since each prime $> k$ can divide at most one term, there are at least $k - \mu$ primes $> k$ dividing Δ'. Thus

$$\omega(\Delta') \geq \pi(k) + k - \mu.$$

Putting $x = n + k - 1$, we see that $\Delta' = \Delta$ and hence

$$\omega(\Delta) \geq \pi(k) + k - \mu$$

and the Theorems 1.2.1 for $k \geq 19$ and Theorem 1.2.4 for $k \geq 10$ follow from (4.1.2) and (4.1.3), respectively.

We give a sketch of the proof of Theorem 4.1.1. We first show that it is enough to prove Theorem 4.1.1 (*a*) for k which are primes and Theorem 4.1.1 (*b*) for k such that $2k - 1$ is prime. The estimates of π function given in Lemma 3.1.2 have been applied to count the number of terms in $\Delta'(x, k)$ which are primes and the number of terms of the form ap with $2 \leq a \leq 6$ and $p > k$. The latter contribution is crucial for keeping the estimates well under computational range. It has been applied in the interval $2k \leq x < 7k$. In fact this interval has been partitioned into several subintervals and it has been applied to each of those subintervals. This leads to sharper estimates. See Lemmas 4.2.6, 4.2.7, 4.2.9. For covering the range $x \geq 7k$, the ideas of Erdős [**10**] have been applied, see Lemmas 4.2.3, 4.2.5, 4.2.8.

4.2. Lemmas

Lemma 4.2.1. *We have*

$$M(k) = \begin{cases} \left[\frac{3}{4}\pi(k)\right] - 1 & \text{if} \quad k \in \mathfrak{K}_1 \\ \pi(2k) - \pi(k) & \text{otherwise} \end{cases} \tag{4.2.1}$$

where $\mathfrak{K}_1$ *is given by*

$$\begin{aligned} \mathfrak{K}_1 = \{&19, 20, 47, 48, 73, 74, 83, 89, 107, 108, 109, 110, 111, 112, 113, 114, \\ &115, 116, 173, 199, 200, 277, 278, 281, 282, 283, 284, 285, 293\}. \end{aligned} \tag{4.2.2}$$

Proof. By Lemma 3.1.2 (i) and (ii), we have

$$\pi(2k) - \pi(k) - \left[\frac{3}{4}\pi(k)\right] + 1 \geq \frac{2k}{\log(2k) - 1} - \frac{7}{4}\frac{k}{\log k}\left(1 + \frac{1.2762}{\log k}\right) + 1$$

for $k \geq 2697$. The right hand side of the above inequality is an increasing function of k and it is non-negative at $k = 2697$. Hence $\pi(2k) - \pi(k) \geq \left[\frac{3}{4}\pi(k)\right] - 1$ for $k \geq 2697$ thereby giving $M(k) = \pi(2k) - \pi(k)$ for $k \geq 2697$. For $k < 2697$, we check that (4.2.1) is valid. □

Lemma 4.2.2. (*i*) *Let* $k' < k''$ *be consecutive primes. Suppose Theorem 4.1.1* **(a)** *holds at* k'. *Then it holds for all* k *with* $k' \leq k < k''$.
(*ii*) *Let* $k_1 < k_2$ *be such that* $2k_1 - 1$ *and* $2k_2 - 1$ *are consecutive primes. Suppose Theorem 4.1.1* **(b)** *holds at* k_1. *Then Theorem 4.1.1* **(b)** *holds for all* k *with* $k_1 \leq k < k_2$, $k \notin \mathfrak{K}_1$.

Proof. For the proof of (4.1.2) and (4.1.3), it suffices to show that

$$W(\Delta') \geq \left[\frac{3}{4}\pi(k)\right] - 1 \tag{4.2.3}$$

and

$$W(\Delta') \geq M(k), \tag{4.2.4}$$

respectively.

Suppose that Theorem 4.1.1 **(a)** holds at k' for k' prime. Let k as in the statement of the Lemma and $x \geq 2k$. Then $x \geq 2k_1$ and $\Delta' = x(x-1)\cdots(x-k'+1)(x-k')\cdots(x-k+1)$. Thus

$$W(\Delta') \geq W(x(x-1)\cdots(x-k'+1)) \geq \left[\frac{3}{4}\pi(k')\right] - 1 = \left[\frac{3}{4}\pi(k)\right] - 1.$$

We now prove (*ii*). Assume that Theorem 4.1.1 **(b)** holds at k_1. Let k be as in the statement of the lemma. Further let $x \geq \frac{29}{12}k - 1 \geq \frac{29}{12}k_1 - 1$. Since $k \notin \mathfrak{K}_1$, we have $M(k) = \pi(2k) - \pi(k)$ by Lemma 4.2.1. Also $\pi(2k_1) = \pi(2k_1 - 1) = \pi(2k - 1) = \pi(2k)$. Therefore

$$W(\Delta') \geq W(x(x-1)\cdots(x-k_1+1)) \geq M(k_1) \geq \pi(2k_1) - \pi(k_1) \geq \pi(2k) - \pi(k) = M(k).$$

□

For the next lemma, we need some notations. Let $P_0 > 0$ and $\nu \geq 0$ with $g_1, g_2, \cdots g_\nu$ be all the integers in $[0, k)$ such that each of $x - g_i$ with $1 \leq i \leq \nu$ is divisible by a prime exceeding P_0. Further we write

$$(x - g_1)\cdots(x - g_\nu) = GH \tag{4.2.5}$$

with $\gcd(G, H) = 1$, $\gcd(H, \prod\limits_{p \leq P_0} p) = 1$. Then we have

Lemma 4.2.3. *If* $x < P_0^{\frac{3}{2}}$, *then*

$$\binom{x}{k} \leq (2.83)^{P_0 + \sqrt{x}} x^\nu \left(G \prod_{p > P_0} p^{\mathrm{ord}_p(k!)}\right)^{-1}. \tag{4.2.6}$$

Proof. We observe that

$$\mathrm{ord}_p\binom{x}{k} = \sum_{\nu=1}^{\infty}\left(\left[\frac{x}{p^\nu}\right] - \left[\frac{x-k}{p^\nu}\right] - \left[\frac{k}{p^\nu}\right]\right).$$

Each of the summand is at most 1 if $p^\nu \le x$ and 0 otherwise. Therefore $\mathrm{ord}_p\binom{x}{k} \le s$ where $p^s \le x < p^{s+1}$. Thus

$$p^{\mathrm{ord}_p\binom{x}{k}} \le p^s \le x. \tag{4.2.7}$$

Therefore

$$\prod_{p\le P_0} p^{\mathrm{ord}_p\binom{x}{k}} \le \prod_{\substack{p\le P_0\\ p^a\le x}} p^a \le \prod_{p\le P_0} p \prod_{p\le x^{\frac{1}{2}}} p \prod_{p\le x^{\frac{1}{3}}} p\cdots. \tag{4.2.8}$$

From Lemma 3.1.1 (iii) with $\nu = \sqrt{x}$ and $\nu = P_0$, we get

$$\prod_{p\le x^{\frac{1}{2}}} p \prod_{p\le x^{\frac{1}{4}}} p \prod_{p\le x^{\frac{1}{6}}} p\cdots. < (2.83)^{\sqrt{x}} \tag{4.2.9}$$

and

$$\prod_{p\le P_0} p \prod_{p\le P_0^{\frac{1}{2}}} p \prod_{p\le P_0^{\frac{1}{3}}} p\cdots. < (2.83)^{P_0},$$

respectively. Since $x < P_0^{\frac{3}{2}}$, we have $P_0^{\frac{1}{l}} > x^{\frac{1}{2l-1}}$ for $l \ge 2$ so that the latter inequality implies

$$\prod_{p\le P_0} \prod_{p\le x^{\frac{1}{3}}} p \prod_{p\le x^{\frac{1}{5}}} p\cdots. < (2.83)^{P_0}. \tag{4.2.10}$$

Combining (4.2.8), (4.2.9) and (4.2.10), we get

$$\prod_{p\le P_0} p^{\mathrm{ord}_p\binom{x}{k}} \le (2.83)^{P_0+\sqrt{x}}. \tag{4.2.11}$$

By (4.2.5), we have

$$\prod_{p> P_0} p^{\mathrm{ord}_p\binom{x}{k}} = \frac{(x-g_1)\cdots(x-g_\nu)}{G\prod_{p>P_0} p^{\mathrm{ord}_p(k!)}}. \tag{4.2.12}$$

Further we observe that

$$(x-g_1)\cdots(x-g_\nu) < x^\nu. \tag{4.2.13}$$

Finally, we combine (4.2.11), (4.2.12) and (4.2.13) to conclude (4.2.6). □

Lemma 4.2.3 with $P_0 = k$ implies the following result immediately, see Saradha and Shorey [**61**, Lemma 3].

Corollary 4.2.4. *Let $x < k^{\frac{3}{2}}$. Assume that* (4.1.1) *holds. Then*

$$\binom{x}{k} \le (2.83)^{k+\sqrt{x}} x^{k-\mu}.$$

Lemma 4.2.5. *Assume* (4.1.1) *and*

$$\mu \ge k - M(k) + 1 \tag{4.2.14}$$

where $M(k)$ is given by (4.1.4). *Then we have*

(*i*) $x < k^{\frac{3}{2}}$ *for* $k \ge 71$
(*ii*) $x < k^{\frac{7}{4}}$ *for* $k \ge 25$
(*iii*) $x < k^2$ *for* $k \ge 13$
(*iv*) $x < k^{\frac{9}{4}}$ *for* $k \ge 10$.

Proof. Since $(x-f_1)\cdots(x-f_\mu)$ divides $\binom{x}{k}k!$, we observe from (4.1.1) and (4.2.7) that

$$(x-f_1)\cdots(x-f_\mu)\le\left(\prod_{p\le k}p^{\mathrm{ord}_p\binom{x}{k}}\right)k!\le\left(\prod_{p\le k}x\right)k!=x^{\pi(k)}k!. \tag{4.2.15}$$

Also

$$(x-f_1)\cdots(x-f_\mu)\ge(x-f_\mu)^\mu\ge(x-k+1)^\mu>x^\mu\left(1-\frac{k}{x}\right)^\mu.$$

Comparing this with (4.2.15), we get

$$k!>x^{\mu-\pi(k)}\left(1-\frac{k}{x}\right)^\mu. \tag{4.2.16}$$

Let $k\ge 71$. We assume that $x\ge k^{\frac{3}{2}}$ and we shall arrive at a contradiction. From (4.2.16), we have

$$k!>k^{\frac{3}{2}(\mu-\pi(k))}\left(1-\frac{1}{\sqrt{k}}\right)^\mu \tag{4.2.17}$$

and since $\mu\le k$,

$$k!>k^{\frac{3}{2}(\mu-\pi(k))}\left(1-\frac{1}{\sqrt{k}}\right)^k. \tag{4.2.18}$$

We use (4.2.18), (4.2.14), (4.2.1) and Lemmas 3.1.2 (i) and 3.1.7 to derive for $k\ge 294$ that

$$1>2.718k^{\frac{1}{2}-\frac{3}{\log 2k}(1+\frac{1.2762}{\log 2k})}(1-\frac{1}{\sqrt{k}})$$

since $\exp\left(\frac{\log 0.3989k}{k}-\frac{1}{12k^2}\right)\ge 1$. The right hand side of above inequality is an increasing function of k and it is not valid at $k=294$. Thus $k\le 293$. Further we check that (4.2.18) is not valid for $71\le k\le 293$ except at $k=71,73$ by using (4.2.14) with $\mu=k-M(k)+1$ and the exact values of $k!$ and $M(k)$. Let $k=71,73$. We check that (4.2.17) is not satisfied if (4.2.14) holds with equality sign. Thus we may suppose that (4.2.14) holds with strict inequality. Then we find that (4.2.18) does not hold. This proves (i). For the proofs of (ii), (iii) and (iv), we may assume that $x\ge k^{\frac{7}{4}}$ for $25\le k\le 70$, $x\ge k^2$ for $13\le k\le 24$ and $x\ge k^{\frac{9}{4}}$ for $k=10,11,12$, respectively, and arrive at a contradiction. □

The next four lemmas show that under the hypothesis of Theorem 4.1.1, k is bounded. Further we show that Theorem 4.1.1 **(a)** is valid for primes k if $x\le\frac{29}{12}k-1$ and Theorem 4.1.1 **(b)** is valid for all $k\in\mathfrak{K}$ where

$$\mathfrak{K}=\mathfrak{K}_1\cup\{k\big|k\ge 10\text{ and }2k-1\text{ is a prime}\}. \tag{4.2.19}$$

Lemma 4.2.6. **(a)** *Let $k\ge 19$ be a prime, $2k\le x\le\frac{29}{12}k-1$ and $(x,k)\notin S_3$. Then Theorem 4.1.1(**a**) is valid.*
(b) *Let $k\ge 10$, $\frac{29}{12}k-1<x<3k$. Then Theorem 4.1.1(**b**) holds for all $k\in\mathfrak{K}$.*

Proof. Let $2k\le x<3k$. We observe that every prime p with $k\le x-k<p\le x$ is a term of Δ'. Since $k>\frac{x-k}{2}$, we also see that $2p$ is a term in Δ' for every prime p with $k<p\le\frac{x}{2}$. Thus

$$W(\Delta')\ge\pi(x)-\pi(x-k)+\pi\left(\frac{x}{2}\right)-\pi(k). \tag{4.2.20}$$

The contribution of $\pi(\frac{x}{2})-\pi(k)$ in the above expression is necessary to get an upper bound for k which is not very large.
(a) Let $2k\le x\le\frac{29}{12}k-1$ with $(x,k)\notin S_3$. We will show that (4.2.3) holds. Let $(2+t_1)k\le x<(2+t_2)k$ with $0\le t_1<t_2\le 1$ and $t_2-t_1\le\frac{1}{4}$. Then we have from (4.2.20) that

$$W(\Delta')\ge\pi(2k+t_1k)-\pi(k+t_2k)+\pi(k+\frac{t_1k}{2})-\pi(k).$$

Hence it is enough to prove

$$\pi((2+t_1)k)-\pi((1+t_2)k)+\pi((1+\frac{t_1}{2})k)-\pi(k)-\left[\frac{3}{4}\,\pi(k)\right]+1\geq 0. \tag{4.2.21}$$

Using Lemma 3.1.2 (i), (ii) and

$$\frac{\log Y}{\log Z}=1+\frac{\log(\frac{Y}{Z})}{\log Z} \text{ and } \frac{\log Y}{\log Z-1}=1+\frac{1+\log(\frac{Y}{Z})}{\log Z-1}\ ,$$

we see that the left hand side of (4.2.21) is at least

$$\begin{aligned}&\sum_{i=1}^{2} b\left(\frac{2+t_1}{i}k\right)-a((1+t_2)k)-\frac{7}{4}\ a(k)+1\\ =&\frac{k}{(\log(2+t_1)k)^2}\left\{f(k,t_1,t_2)-g(k,t_1,t_2)-\frac{7}{4}g(k,t_1,0)\right\}+1\end{aligned} \tag{4.2.22}$$

for $k\geq 5393$, where

$$f(k,t_1,t_2)=(1.5t_1-t_2+\frac{1}{4})(\log(2+t_1)k)+\sum_{i=1}^{2}\frac{(2+t_1)(1+\log i)}{i}\left(1+\frac{1+\log i}{\log((2+t_1)k/i)-1}\right)$$

and

$$g(k,t_1,t_2)=(1+t_2)\left(1+\frac{\log(\frac{2+t_1}{1+t_2})}{\log((1+t_2)k)}\right)\left(1.2762+\log\left(\frac{2+t_1}{1+t_2}\right)+\frac{1.2762\log(\frac{2+t_1}{1+t_2})}{\log((1+t_2)k)}\right).$$

Then we have

$$kf'(k,t_1,t_2)=(1.5t_1-t_2+\frac{1}{4})-\sum_{i=1}^{2}\left(\frac{2+t_1}{i}\right)\left(\frac{1+\log i}{\log((2+t_1)k/i)-1}\right)^2.$$

We write

$$1.5t_1-t_2+\frac{1}{4}=0.5t_1-(t_2-t_1)+\frac{1}{4}$$

to observe that the left hand side is positive unless $(t_1,t_2)=(0,\frac{1}{4})$ and we shall always assume that $(t_1,t_2)\neq(0,\frac{1}{4})$.

Let $k_0=k_0(t_1,t_2)$ be such that $kf'(k,t_1,t_2)$ is positive at k_0. Since $kf'(k,t_1,t_2)$ is an increasing function of k, we see that $f(k,t_1,t_2)$ is also an increasing function of k for $k\geq k_0$. Also $g(k,t_1,t_2)$ is a decreasing function of k. Hence (4.2.22) is an increasing function of k for $k\geq k_0$. Let $k_1=k_1(t_1,t_2)\geq k_0$ be such that (4.2.22) is non-negative at k_1. Then (4.2.21) is valid for $k\geq k_1$. For $k<k_1$, we check inequality (4.2.21) by using the exact values of $\pi(\nu)$. Again for k not satisfying (4.2.21), we take $x=2k+r$ with $t_1k\leq r<t_2k$ and check that the right hand side of (4.2.20) is at least the right hand side of (4.2.3).

Let $2k\leq x<\frac{49}{24}k$. Then $t_1=0,t_2=\frac{1}{24}$ and we find $k_1=5393$ by (4.2.22). For $k<5393$ and k prime, we check that (4.2.21) holds except at the following values of k:

$$\begin{cases}19,47,71,73,83,89,103,107,109,113,151,167,173,191,193,197,\\199,269,271,277,281,283,293,449,463,467,491,503,683,709.\end{cases}$$

Thus (4.2.3) is valid for all primes k except at above values of k. For these values of k, we take $x=2k+r$ with $0\leq r<\frac{k}{24}$ and show that the right hand side of (4.2.20) is at least the right hand side of (4.2.3) except at $(x,k)\notin S_3$.

We divide the interval $[\frac{49}{24}k,\frac{29}{12}k)$ into following subintervals

$$\left[\frac{49}{24}k,\frac{25}{12}k\right),\ \left[\frac{25}{12}k,\frac{13}{6}k\right),\ \left[\frac{13}{6}k,\frac{9}{4}k\right),\ \left[\frac{9}{4}k,\frac{19}{8}k\right) \text{ and } \left[\frac{19}{8}k,\frac{29}{12}k\right).$$

We find $k_1 = 5393$ for each of these intervals. For $k < 5393$ and k prime, we check that (4.2.21) holds except at following values of k for the intervals:

$$\left[\frac{49}{24}k, \frac{25}{12}k\right) : \begin{cases} 19, 47, 67, 71, 73, 79, 83, 103, 107, 109, 113, 131, 151, 167, 181, 199, \\ 211, 263, 271, 277, 293, 467, 683 \end{cases}$$

$$\left[\frac{25}{12}k, \frac{17}{8}k\right) : \Big\{ 19, 71, 83, 101, 103, 107, 113, 179, 181, 199, 257, 281, 283, 467, 683$$

$$\left[\frac{17}{8}k, \frac{13}{6}k\right) : \Big\{ 19, 37, 47, 61, 73, 89, 113, 197$$

$$\left[\frac{13}{6}k, \frac{9}{4}k\right) : \Big\{ 19, 43, 61, 67, 83, 89, 113, 139, 193, 197, 199, 257, 281, 283$$

$$\left[\frac{9}{4}k, \frac{19}{8}k\right) : \begin{cases} 19, 23, 31, 43, 47, 61, 79, 83, 109, 113, 139, 151, 167, 193, 197, 199, \\ 239, 283, 359 \end{cases}$$

and there are no exceptions for the subinterval $\left[\frac{19}{8}k, \frac{29}{12}k\right)$. Now we apply similar arguments as in the case $2k \le x < \frac{49}{24}k$ to each of the above subintervals to complete the proof.

For the proof of **(b)**, we divide $\frac{29}{12}k - 1 < x < 3k$ into subintervals $\left(\frac{29}{12}k - 1, \frac{5}{2}k\right)$, $\left[\frac{5}{2}k, \frac{21}{8}k\right)$, $\left[\frac{21}{8}k, \frac{11}{4}k\right)$ and $\left[\frac{11}{4}k, 3k\right)$. We apply the arguments of **(a)** to each of these subintervals to conclude that the right hand side of (4.2.20) is at least the right hand side of (4.2.4). Infact we have the inequality

$$\pi((2+t_1)k) - \pi((1+t_2)k) + \pi((1+\frac{t_1}{2})k) - \pi(k) - M(k) \ge 0 \tag{4.2.23}$$

analogous to that of (4.2.21). As in **(a)**, using (4.2.1), we derive that $k_1 = 5393$ in each of these intervals. For $k < 5393$ and $k \in \mathfrak{K}$, we check that (4.2.23) hold except at the following values of k for the intervals:
$\left(\frac{29}{12}k - 1, \frac{5}{2}k\right)$: $\{54, 55, 57, 73, 79, 142\}$,
$\left[\frac{5}{2}k, \frac{21}{8}k\right)$: $\{12, 52, 55, 70\}$,
$\left[\frac{21}{8}k, \frac{11}{4}k\right)$: $\{22, 27\}$
$\left[\frac{11}{4}k, 3k\right)$: $\{10, 12, 19, 21, 22, 24, 37, 54, 55, 57, 59, 70, 91, 100, 121, 142, 159\}$.
Now we proceed as in **(a)** to get the required result. □

LEMMA 4.2.7. *Let $k \in \mathfrak{K}$ and $3k \le x < 7k$. Then Theorem 4.1.1* **(b)** *is valid.*

We prove a stronger result that Theorem 4.1.1 **(b)** holds for all $k \ge 29000$ and for $k \in \mathfrak{K}$.

PROOF. Let $3k \le x < 7k$. We show that (4.2.4) holds. Let $(s+t_1)k \le x < (s+t_2)k$ with integers $3 \le s \le 6$ and $t_1, t_2 \in \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}$ such that $t_2 - t_1 = \frac{1}{4}$. Then Δ' contains a term equal to ip with $\frac{x-k}{i} < p \le \frac{x}{i}$ for each i with $1 \le i < s$ and a term equal to sp for $k < p \le \frac{x}{s}$. Therefore

$$W(\Delta') \ge \sum_{i=1}^{s-1} \left(\pi\left(\frac{x}{i}\right) - \pi\left(\frac{x-k}{i}\right) \right) + \pi\left(\frac{x}{s}\right) - \pi(k). \tag{4.2.24}$$

Since $x \ge (s+t_1)k$ and $x - k < (s-1+t_2)k$, we observe from (4.2.24) that

$$W(\Delta') \ge \sum_{i=1}^{s-1} \left(\pi\left(\frac{s+t_1}{i}k\right) - \pi\left(\frac{s-1+t_2}{i}k\right) \right) + \pi\left(\frac{s+t_1}{s}k\right) - \pi(k).$$

Hence it is enough to show

$$\sum_{i=1}^{s-1} \left(\pi\left(\frac{s+t_1}{i}k\right) - \pi\left(\frac{s-1+t_2}{i}k\right) \right) + \pi\left(\frac{s+t_1}{s}k\right) - \pi(k) - M(k) \ge 0. \tag{4.2.25}$$

Using (4.2.1) and Lemma 3.1.2 (i), (ii), we see that the left hand side of (4.2.25) is at least

$$\begin{aligned}&\sum_{i=1}^{s-1}\left(b\left(\frac{s+t_1}{i}k\right)-a\left(\frac{s-1+t_2}{i}k\right)\right)+b\left(\frac{s+t_1}{s}k\right)-a(2k)\\ =&\frac{k}{(\log(s+t_1)k)^2}\left\{F(k,s,t_1,t_2)-\sum_{i=1}^{s-1}G(k,s,t_1,t_2,i)-G(k,s,t_1,1,\frac{s}{2})\right\}\end{aligned}\tag{4.2.26}$$

for $k \geq 5393$, where

$$\begin{aligned}F(k,s,t_1,t_2)=&\left(\sum_{i=1}^{s-1}\left(\frac{1+t_1-t_2}{i}\right)+\frac{t_1}{s}-1\right)(\log(s+t_1)k)+\\ &+\sum_{i=1}^{s}\frac{(s+t_1)(1+\log i)}{i}\left(1+\frac{1+\log i}{\log((s+t_1)k/i)-1}\right)\end{aligned}$$

and

$$\begin{aligned}G(k,s,t_1,t_2,i)=&\left(\frac{s-1+t_2}{i}\right)\left(1+\frac{\log\left(\frac{(s+t_1)i}{s-1+t_2}\right)}{\log\left(\frac{s-1+t_2}{i}k\right)}\right)\times\\ &\left(1.2762+\log\left(\frac{(s+t_1)i}{s-1+t_2}\right)+\frac{1.2762\log\left(\frac{(s+t_1)i}{s-1+t_2}\right)}{\log\left(\frac{s-1+t_2}{i}k\right)}\right).\end{aligned}$$

Then

$$kF'(k,s,t_1,t_2)=\left(\sum_{i=1}^{s-1}\left(\frac{1+t_1-t_2}{i}\right)+\frac{t_1}{s}-1\right)-\sum_{i=1}^{s}\frac{(s+t_1)}{i}\left(\frac{1+\log i}{\log((s+t_1)k/i)-1}\right)^2.$$

If $s = 2$, we note that F and G are functions similar to f and g appearing in Lemma 4.2.6. As in Lemma 4.2.6, we find $K_1 := K_1(s, t_1, t_2)$ such that (4.2.26) is non negative at $k = K_1$ and it is increasing for $k \geq K_1$. Hence (4.2.25) is valid for $k \geq K_1$. For $k < K_1$, we check inequality (4.2.25) by using the exact values of π function in (4.2.25) for k with $2k - 1$ prime or primes k given by (4.2.2). Again for k not satisfying (4.2.25), we take $x = sk + r$ with $t_1 k \leq r < t_2 k$ and check that the right hand side of (4.2.24) is at least the right hand side of (4.2.4).

Let $3k \leq x < \frac{13}{4}k$. Here $t_1 = 0,\ t_2 = \frac{1}{4}$ and and we find $K_1 = 29000$. We check that (4.2.25) holds for $3 \leq k < 29000$ except at $k = 10, 12, 19, 22, 40, 42, 52, 55, 57, 100, 101,\ 126, 127, 142$. For these values of k, putting $x = 3k + r$ with $0 \leq r < \frac{1}{4}k$, we show that the right hand side of (4.2.24) is at least the right hand side of (4.2.4). Hence the assertion follows in $3k \leq x < \frac{13}{4}k$. For $x \geq \frac{13}{4}k$, we apply similar arguments to intervals $(s + t_1)k \leq x < (s + t_2)k$ with integers $3 \leq s \leq 6$ and $t_1, t_2 \in \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}$ such that $t_2 - t_1 = \frac{1}{4}$. We find $K_1 = 5393$ for each of these intervals except for $6k \leq x < \frac{25}{4}k$ where $K_1 = 5500$. □

In view of Lemmas 4.2.6 and 4.2.7, it remains to prove Theorem 4.1.1 for $x \geq 7k$ which we assume. Further we may also suppose (4.2.14). Otherwise (4.1.3) follows. Now we derive from Lemma 4.2.5 that $x < k^{\frac{9}{4}}$. On the other hand, we prove $x \geq k^{\frac{9}{4}}$. This is a contradiction. We split the proof of $x \geq k^{\frac{9}{4}}$ in the following two lemmas.

LEMMA 4.2.8. *Let $k \in \mathfrak{K}$. Assume* (4.1.1), (4.2.14) *with $x \geq 7k$. Then $x \geq k^{\frac{3}{2}}$.*

PROOF. We prove it by contradiction. We assume (4.1.1), (4.2.14) and $7k \leq x < k^{\frac{3}{2}}$. Then $k \geq 50$. Further by Corollary 4.2.4 and $\binom{x}{k} \geq \binom{7k}{k}$, we have

$$\binom{7k}{k} < (2.83)^{k+k^{\frac{3}{4}}} k^{\frac{3}{2}(M(k)-1)}\tag{4.2.27}$$

since $x < k^{\frac{3}{2}}$. We observe from Lemma 3.1.7 that

$$\begin{aligned}\binom{7k}{k} = \frac{(7k)!}{k!(6k)!} &> \frac{\sqrt{14\pi k}\exp^{-7k}(7k)^{7k}\exp^{\frac{1}{84k+1}}}{\sqrt{2\pi k}\exp^{-k}k^k\exp^{\frac{1}{12k}}\sqrt{12\pi k}\exp^{-6k}(6k)^{6k}\exp^{\frac{1}{72k}}} \\ &> \frac{0.4309}{\sqrt{k}}\exp^{\frac{1}{84k+1}-\frac{7}{72k}}(17.65)^k.\end{aligned}$$

Combining this with (4.2.27), we get

$$1 > \exp\left(\log(0.4309k) + \frac{1}{84k+1} - \frac{7}{72k}\right)(17.65)^k(2.83)^{-k-k^{\frac{3}{4}}}k^{-\frac{3}{2}M(k)}. \tag{4.2.28}$$

Using (4.2.1), Lemma 1(i), (ii) and $\exp\left(\frac{\log(0.4309k)}{k} + \frac{1}{84k^2+k} - \frac{7}{72k^2}\right) \geq 1$, we derive for $k \geq 5393$ that

$$\begin{aligned}1 &> 6.2367(2.83)^{-k^{-\frac{1}{4}}}k^{-\frac{3}{\log 2k}(1+\frac{1.2762}{\log 2k})+\frac{3}{2(\log k-1)}} \\ &> 6.2367\exp\left(\frac{3}{2} + \frac{3}{2\log k - 2}\right)(2.83)^{-k^{-\frac{1}{4}}}k^{-\frac{3}{\log 2k}(1+\frac{1.2762}{\log 2k})} \\ &> 27.95(2.83)^{-k^{-\frac{1}{4}}}k^{-\frac{3}{\log 2k}(1+\frac{1.2762}{\log 2k})} := h(k)\end{aligned}$$

since $\exp\left(\frac{3}{2\log k-2}\right) > 1$ for $k \geq 3$. We see that $h(k)$ is an increasing function of k and $h(k) > 1$ at $k = 5393$. Therefore $k < 5393$. By using the exact values of $M(k)$, we now check that (4.2.28) does not hold for $50 \leq k < 5393$ and $k \in \mathfrak{K}$. □

Lemma 4.2.9. *Let $k \in \mathfrak{K}$. If (4.1.1) and (4.2.14) hold and $x \geq k^{\frac{3}{2}}$, then $x \geq k^{\frac{9}{4}}$.*

Proof. We prove by contradiction. Assume (4.1.1), (4.2.14) and $k^{\frac{3}{2}} \leq x < k^{\frac{9}{4}}$. We derive from Lemma 4.2.5 that $k \leq 70$. Let $k = 10, 11, 12, 13$. By Lemmas 4.2.5, 4.2.7 and 4.2.8, we can take $\max(7k, k^{\frac{3}{2}}) \leq x < k^{\frac{9}{4}}$ for $k = 10, 11, 12$ and $\max(7k, k^{\frac{3}{2}}) \leq x < k^2$ for $k = 13$. For these values of x and k, we find that

$$W(\Delta') \geq \sum_{i=1}^{6}\left(\pi\left(\frac{x}{i}\right) - \pi\left(\frac{x-k}{i}\right)\right) \geq M(k)$$

contradicting (4.2.14).

Therefore we assume that $k \geq 14$. Let $k^{\frac{3}{2}} \leq x < k^{\frac{25}{16}}$. By Lemma 4.2.7 and 4.2.8, we can take $x \geq \max(7k, k^{\frac{3}{2}})$ so that we can assume $k \geq 32$. Then

$$\binom{x}{k} \geq \binom{\max(7k, \lceil k^{\frac{3}{2}}\rceil)}{k}$$

where $\lceil \nu \rceil$ denotes the least integer $\geq \nu$. From (4.2.7), we have $\mathrm{ord}_p(\binom{x}{k}) \leq \left[\frac{\log\ x}{\log\ p}\right] \leq \left[\frac{25}{16}\frac{\log\ k}{\log\ p}\right]$ and hence

$$\binom{x}{k} \leq \left(\prod_{i=1}^{\pi(k)} p_i^{\left[\frac{25}{16}\frac{\log\ k}{\log\ p_i}\right]}\right)x^{k-\mu} < \left(\prod_{i=1}^{\pi(k)} p_i^{\left[\frac{25}{16}\frac{\log\ k}{\log\ p_i}\right]}\right)k^{\frac{25}{16}(M(k)-1)}$$

by (4.2.14). Combining the above estimates for $\binom{x}{k}$, we get

$$\binom{\max(7k, \lceil k^{\frac{3}{2}}\rceil)}{k} < \left(\prod_{i=1}^{\pi(k)} p_i^{\left[\frac{25}{16}\frac{\log\ k}{\log\ p_i}\right]}\right)k^{\frac{25}{16}(M(k)-1)}$$

which is not possible for $32 \leq k \leq 70$. By similar arguments, we arrive at a contradiction for $\max(7k, k^{\frac{25}{16}}) \leq x < k^{\frac{26}{16}}$ in $23 \leq k \leq 70$, $\max(7k, k^{\frac{26}{16}}) \leq x < k^{\frac{27}{16}}$ in $17 \leq k \leq 70$ and $\max(7k, k^{\frac{27}{16}}) \leq$

$x < k^{\frac{7}{4}}$ in $14 \leq k \leq 70$ except at $k = 16$. Let $k = 16$ and $\max(7k, k^{\frac{27}{16}}) \leq x < k^{\frac{7}{4}}$. Then we observe that

$$W(\Delta') \geq \sum_{i=1}^{6} \left(\pi\left(\frac{x}{i}\right) - \pi\left(\frac{x-16}{i}\right)\right) \geq 5 = M(16)$$

contradicting (4.2.14).

Now we consider $x \geq k^{\frac{7}{4}}$. We observe that $k^{\frac{7}{4}} \geq 7k$ since $k \geq 14$. Further we derive from Lemma 4.2.5 that $k \leq 24$. We apply similar arguments for $14 \leq k \leq 24$ as above to arrive at a contradiction in the intervals $k^{\frac{7}{4}} \leq x < k^{\frac{15}{8}}$ except at $k = 16$, $k^{\frac{15}{8}} \leq x < k^{\frac{31}{16}}$ and $k^{\frac{31}{16}} \leq x < k^2$. The case $k = 16$ and $k^{\frac{7}{4}} \leq x < k^{\frac{15}{8}}$ is excluded as earlier. □

4.3. Proof of Theorem 4.1.1

Suppose that the hypothesis of Theorem 4.1.1 **(b)** is valid and $k \geq 10$. By Lemmas 4.2.6 **(b)**, 4.2.7, 4.2.8 and 4.2.9, we see that Theorem 4.1.1 **(b)** is valid for all $k \in \mathfrak{K}$. Thus (4.2.4) holds for all $k \in \mathfrak{K}$ and $x > \frac{29}{12}k - 1$. Let $k \notin \mathfrak{K}$ and $k_1 < k$ be the largest integer with $2k_1 - 1$ prime. Then $k_1 \geq 10$. For $x > \frac{29}{12}k - 1 > \frac{29}{12}k_1 - 1$, we see that (4.2.4) is valid at (x, k_1). By Lemma 4.2.2 (*ii*), (4.2.4) is valid at (x, k) too. Hence Theorem 4.1.1 **(b)** is valid for all k.

Suppose that the hypothesis of Theorem 4.1.1 are satisfied and $k \geq 19$. We have from Lemma 4.2.6 **(a)** that (4.2.3) holds for (x, k) with k prime, $x \leq \frac{29}{12}k - 1$ and $(x, k) \notin S_3$. By Theorem 4.1.1(**b**), (4.2.4) and hence (4.2.3) is valid for all k and $x > \frac{29}{12}k - 1$. Thus (4.2.3) holds for (x, k) with k prime and $(x, k) \notin S_3$. Let k be a composite number and $k' < k$ be the greatest prime. Then $k' \geq 19$. Suppose $(x, k') \notin S_3$. Then (4.2.3) is valid at (x, k') and hence valid at (x, k) by Lemma 4.2.2 (*i*). Suppose now that $(x, k') \in S_3$. Then we check the validity of (4.2.3) at (x, k). We see that (4.2.3) does not hold only if $(x, k) \in S_3$. We explain this with two examples. Let $k = 20$. Then $k' = 19$. Since $(42, 19) \in S_3$, we check the validity of (4.2.3) at $(42, 20)$ which is true. Hence $(42, 20) \notin S_3$. Again let $k = 72$. Then $k' = 71$. Since $(145, 71) \in S_3$, we check the validity of (4.2.3) at $(145, 72)$ and see that (4.2.3) does not hold at $(145, 72)$ which is an element of S_3. This completes the proof. □

CHAPTER 5

Grimm's Conjecture for consecutive integers: Proof of Theorem 1.2.6

In this chapter, we prove Theorem 1.2.6.

5.1. Introduction

We recall that $N_0 = 8.5 \times 10^8$. For the proof of Theorem 1.2.6, it suffices to prove the following.

THEOREM 5.1.1.

Grimm's Conjecture is valid when $n = p_N + 1$ and $k = k(N) = p_{N+1} - p_N - 1$ for $1 < N \leq N_0$.

For the proof of Theorem 5.1.1, we verify the conjecture of Cramer whenever $N \leq N_0$. We have

LEMMA 5.1.2. *Let $k(N) = p_{N+1} - p_N - 1$. Then*

$$k(N) < (\log p_N)^2 \text{ for } N \leq N_0. \tag{5.1.1}$$

We observe that (5.1.1) can be sharpened for several values of N and this is important for the value of N_0 in Theorem 1.2.6. We also apply the following result of Phillip Hall [**22**] on distinct representations.

LEMMA 5.1.3. *A family $\mathfrak{F} = \{S_i : i \in I\}$ of finite subsets of a set E possesses a system of distinct representatives if and only if for every finite subset J if I, the number of elements in J does not exceed the number of elements of in the set $\cup_{j \in J} S_j$.*

5.2. Proof of Theorem 5.1.1

Let $1 < N \leq N_0$. We put $n = p_N + 1$ and $k = k(N) = p_{N+1} - p_N - 1$. We check that Theorem 5.1.1 is valid for $N \leq 9$. Thus we may suppose that $10 \leq N \leq N_0$. Assume that the assertion of Theorem 5.1.1 is not valid. Now we apply Lemma 5.1.3. Since Grimm's conjecture is not valid, we derive from Lemma 5.1.3 that there exists $t > 0$ and integers $p_N < n_0 < n_1 < \cdots < n_t < n + k = P_{N+1}$ with

$$\omega(n_0 n_1 \cdots n_t) \leq t. \tag{5.2.1}$$

Let $t = t(N)$ be minimal in the above assertion. Then $P(n_i) < k$ for $0 \leq i \leq t$ and (5.2.1) holds with equality sign. We apply a fundamental argument of Sylvester and Erdős. For every prime divisor p of $n_0 n_1 \cdots n_t$, we take an n_{i_p} such that p does not appear to a higher power in the factorisation of any element of $\{n_0, n_1, \cdots, n_t\} =: S$. By deleting all n_{i_p} with p dividing $n_0 n_1 \cdots n_t$ in S, we are left with at least one $n_{i_0} \in S$. If p^ν is the highest power of a prime p dividing n_{i_0}, then p^ν also divides n_{i_p} and hence it divides $|n_{i_0} - n_{i_p}| < k$. Therefore

$$p_N < n_{i_0} < k^t \tag{5.2.2}$$

since $\omega(n_{i_0}) \leq t$. By Lemma 5.1.2, we get

$$\frac{\log p_N}{\log\log p_N} < 2t(N). \tag{5.2.3}$$

We see that the left hand side of (5.2.3) is an increasing function of N. For $i \geq 2$, let N_i be the largest integer N such that

$$\frac{\log p_N}{\log\log p_N} < 2i.$$

Then we calculate

$$N_2 = 727,\ N_3 = 1514619,\ N_4 = 8579289335. \tag{5.2.4}$$

Let A_r and M_r be defined by

$$A_{2r-1} = \prod_{p^\alpha < 2r-1 \le p^{\alpha+1}} p^\alpha,\ M_{2r-1} = \pi(A_{2r-1}).$$

Then

LEMMA 5.2.1. *Suppose that Theorem 5.1.1 is not valid at N with $N > M_{2r-1}$. Then $k(N) > 2r-1$.*

PROOF. Assume that $k(N) = p_{N+1} - p_N - 1 \le 2r-1$. Since Theorem 5.1.1 is not valid, (5.2.1) holds for some t and hence there exists a term $\bar{n}$ such that

$$p_N < \bar{n} \le A_{2r-1}.$$

This is a contradiction since $N > M_{2r-1}$. □

We compute M_{2r-1} for some values of r :

$$M_{11} = 368, M_{13} = 3022, M_{15} = 30785, M_{17} = 58083, M_{19} = 803484,$$
$$M_{21} = M_{23} = 12787622, M_{25} = 250791570.$$

Let

$$S_N = \{p_N + i : P(p_N + i) < k, 1 \le i \le k\}$$

and put $t' = t'(N) = |S_N|$. We see that $t' \ge t+1$. For the proof of Theorem 5.1.1, it suffices to find distinct prime divisors of the elements of S_N since a prime $\ge k$ divides at most one $p_N + i$ with $1 \le i \le k$.

First we consider $N \le N_2$. Let $t = 1$. Then there are $1 \le j < i \le k$ and a prime p such that $p_N + i = p^\alpha$ and $p_N + j = p^\beta$. This gives

$$p_N + j = p^\beta \le p^\beta(p^{\alpha-\beta} - 1) = i - j < k = p_{N+1} - p_N - 1$$

implying $2p_N < p_{N+1} - 1$, a contradiction. Let $t = 2$. Then (5.2.2) holds only when $N = 30$. We have $S_{30} = \{120, 121, 125, 126\}$ and we choose $3, 11, 5$ and 7 as distinct prime divisors of $120, 121, 125$ and 126, respectively. Therefore the assertion of Theorem 5.1.1 holds for $N = 30$. Thus $t \ge 3$ implying $t' \ge t + 1 \ge 4$. Now, by calculating t', we see that $N = 30, 99, 217, 263, 327, 367, 457, 522, 650$ and we verify the assertion of Theorem 5.1.1 as above in each of these values of N.

Hence $N > N_2$. Therefore $t \ge 3$ by the definition of N_2 and thus $t' \ge 4$. Next we consider $N_2 < N \le N_3$. We divide this interval into the following subintervals:

$$I_{11} = (N_2, M_{13}], I_{13} = (M_{13}, M_{15}], I_{15} = (M_{15}, M_{17}], I_{17} = (M_{17}, M_{19}], I_{19} = (M_{19}, N_3].$$

By Lemma 5.2.1, we restrict to those N for which $k(N) > 2r-1$ whenever $N \in I_{2r-1}$ with $6 \le r \le 10$. Let $t = 3$. By (5.2.2) and $t' \ge 4$, we find that N is one of the following:

$$\begin{aligned}
&757, 1183, 1229, 1315, 1409, 1831, 1879, 2225, 2321, 2700, 2788, 2810, 3302, 3385,\\
&3427, 3562, 3644, 3732, 3793, 3795, 3861, 4009, 4231, 4260, 4522, 4754, 5349, 5949,\\
&6104, 6880, 9663, 9872, 10229, 10236, 11214, 11684, 12542, 14357, 14862, 15783,\\
&16879, 17006, 17625, 18266, 19026, 19724, 23283, 23918, 25248, 28593, 31545, 31592,\\
&33608, 34215, 38590, 40933, 44903, 47350, 66762, 104071, 118505, 126172, 141334, 149689.
\end{aligned}$$

Let $P(S_N) = \{P(p_N + i) : p_N + i \in S_N\}$. For the proof of Theorem 5.1.1, we may suppose that

$$|P(S_N)| < |S_N|. \tag{5.2.5}$$

In view of (5.2.5), all above possibilities for N other than the following are excluded:

$$\begin{aligned}
&1409, 1831, 2225, 2788, 3302, 3385, 3562, 3644, 4522,\\
&14862, 16879, 17006, 23283, 28593, 34215, 104071.
\end{aligned} \tag{5.2.6}$$

Let N be given by (5.2.6). We check that $|P(S_N)| = |S_N| - 1$. Let (i, j) with $i < j$ be the unique pair satisfying $P(p_N + i) = P(p_N + j)$. We check that $\omega(p_N + i) \geq 2$. Now we take $P_\mu = P(p_N + \mu)$ if $\mu \neq i$ and P_i to be the least prime divisor of $p_N + i$. Thus all the possibilities in (5.2.6) are excluded. Therefore $t \geq 4$ implying $t' \geq 5$. If $p_N < k^3$, then N is already excluded. Consequently we suppose that $p_N \geq k^3$. Now we calculate t' to find that N is one of the following:

$$\begin{gathered}11159, 19213, 30765, 31382, 40026, 42673, 51943, 57626, 65274, 65320, 80413,\\ 81426, 88602, 106286, 184968, 189747, 192426, 212218, 245862, 256263, 261491,\\ 271743, 278832, 286090, 325098, 327539, 405705, 415069, 435081, 484897, 491237,\\ 495297, 524270, 528858, 562831, 566214, 569279, 629489, 631696, 822210, 870819,\\ 894189, 938452, 1036812, 1150497, 1178800, 1319945, 1394268, 1409075.\end{gathered}$$

By (5.2.5), it suffices to restrict N to

$$57626, 65320, 80413, 106286, 271743, 415069, 822210.$$

These cases are excluded as in (5.2.6).

Thus we may assume that $N > N_3$. Then $t \geq 4$ by the definition of N_3 and $t' \geq 5$. We divide the interval $(N_3, N_0]$ into the following subintervals:

$$J_{19} = (N_3, M_{23}], J_{23} = (M_{23}, N_0].$$

By Lemma 5.2.1, we restrict to those N for which $k(N) > 2r - 1$ whenever $N \in J_{2r-1}$, $r = 10, 12$. By calculating t', we find that N is one of the following:

$$\begin{gathered}1515930, 1539264, 1576501, 1664928, 2053917, 2074051, 2219883, 2324140,\\ 2341680, 2342711, 2386432, 2775456, 2886673, 3237613, 3695514, 5687203,\\ 6169832, 6443469, 6860556, 7490660, 7757686, 8720333, 9558616, 10247124,\\ 10600736, 10655462, 11274670, 11645754, 12672264, 13377906, 14079145,\\ 14289335, 18339279, 24356055, 28244961, 33772762, 42211295, 53468932,\\ 64955634, 110678632, 118374763, 231921327, 264993166, 398367036.\end{gathered}$$

By (5.2.5), it suffices to consider only the following values of N :

$$1539264, 2053917, 2775456, 12672264, 110678632$$

which are excluded as in (5.2.6). This completes the proof of Theorem 5.1.1. □

CHAPTER 6

Refinement of Sylvester's theorem on the greatest prime divisor of a product of consecutive integers: Proof of Theorems 1.3.1, 1.3.3 and Corollary 1.3.2

In this chapter we prove Theorems 1.3.1, 1.3.3 and Corollary 1.3.2. We give a sketch of the proof. For $k = 2, 4$, we use a particular case of Catalan's equation to get the assertion. For $k = 3$ and $5 \le k \le 8$, we use estimates on $\omega(\Delta(n, k)$ given by (1.2.3). For $9 \le k \le 16$, we first bound n and the assertion follows by a computational argument. For $k > 17$, we use arguments similar to that of proving Theorem 1.2.1 and the number of primes in intervals $(X, (1 + \theta)X]$ with $0 < \theta < e - 1$.

6.1. Lemmas

We begin with a well known result due to Levi ben Gerson on a particular case of Catalan equation.

Lemma 6.1.1. *The solutions of*

$$2^a - 3^b = \pm 1 \text{ in integers } a > 0, b > 0$$

are given by $(a, b) = (1, 1), (2, 1), (3, 2)$.

Lemma 6.1.2. *We have*

$$p_{i+1} - p_i < \begin{cases} 35 & \text{for } p_i \le 5591 \\ 15 & \text{for } p_i \le 1123, p_i \ne 523, 887, 1069 \\ 21 & \text{for } p_i = 523, 887, 1069 \\ 9 & \text{for } p_i \le 361, p_i \ne 113, 139, 181, 199, 211, 241, 283, 293, 317, 337. \end{cases} \tag{6.1.1}$$

Lemma 6.1.3. *Let* $\mathfrak{N}$ *be a positive real number and* k_0 *a positive integer. Let* $I(\mathfrak{N}, k_0) = \{i | p_{i+1} - p_i \ge k_0, p_i \le \mathfrak{N}\}$. *Then*

$$P(n(n + 1) \cdots (n + k - 1)) > 2k$$

for $2k \le n < \mathfrak{N}$ *and* $k \ge k_0$ *except possibly when* $p_i < n < n + k - 1 < p_{i+1}$ *for* $i \in I(\mathfrak{N}, k_0)$.

Proof. Let $2k \le n < \mathfrak{N}$ and $k > k_0$. We may suppose that none of $n, n + 1, \cdots, n + k - 1$ is a prime, otherwise the result follows. Let $p_i < n < n + k - 1 < p_{i+1}$. Then $i = \pi(n)$ and $p_{\pi(n)} < n < \mathfrak{N}$. For $\pi(n) \notin I(\mathfrak{N}, k_0)$, we have

$$k - 1 = n + k - 1 - n < p_{\pi(n)+1} - p_{\pi(n)} < k_0$$

which implies $k - 1 < k_0 - 1$, a contradiction. Hence the assertion. □

Lemma 6.1.4. *Let* $X > 0$ *and* $0 < \theta < e - 1$ *be real numbers. For* $l \ge 0$, *let*

$$X_0 = \max\left(\frac{5393}{1+\theta}, \exp(\frac{\log(1+\theta) + 0.2762}{\theta})\right),$$

$$X_{l+1} = \max\left(\frac{5393}{1+\theta}, \exp(\frac{\log(1+\theta) + 0.2762)}{\theta + \frac{1.2762(1-\log(1+\theta))}{\log^2 X_l}})\right).$$

Then we have

$$\pi((1 + \theta)X) - \pi(X) > 0$$

for $X > X_l$.

Proof. Let $l \geq 0$ and $X > X_l$. Then $(1+\theta)X \geq 5393$. By Lemma 3.1.2, we have

$$\begin{aligned}\delta := \pi((1+\theta)X) - \pi(X) &\geq \frac{(1+\theta)X}{\log(1+\theta)X - 1} - \frac{X}{\log X}\left(1 + \frac{1.2762}{\log X}\right)\\ &\geq \frac{X}{\log(1+\theta)X - 1}\left\{1+\theta - \frac{\log(1+\theta)X-1}{\log X}\left(1+\frac{1.2762}{\log X}\right)\right\}\\ &\geq \frac{X}{\log(1+\theta)X - 1}\left\{1+\theta - \left(1 - \frac{1-\log(1+\theta)}{\log X}\right)\left(1+\frac{1.2762}{\log X}\right)\right\}\\ &\geq \frac{X}{\log(1+\theta)X - 1}\left\{F(X)+G(X)\right\}\end{aligned}$$

where $F(X) = \theta - \frac{\log(1+\theta)+0.2762}{\log X}$ and $G(X) = \frac{1.2762(1-\log(1+\theta))}{\log^2 X}$. We see that $G(X) > 0$ and decreasing since $0 < \theta < e-1$. Further we observe that $\{X_i\}$ is a non-increasing sequence. We notice that $\delta > 0$ if $F(X)+G(X) > 0$. But $F(X)+G(X) > F(X) > 0$ for $X > X_0$ by the definition of X_0. Thus $\delta > 0$ for $X > X_0$. Let $X \leq X_0$. Then $F(X)+G(X) \geq F(X)+G(X_0)$ and $F(X)+G(X_0) > 0$ if $X > X_1$ by the definition of X_1. Hence $\delta > 0$ for $X > X_1$. Now we proceed inductively as above to see that $\delta > 0$ for $X > X_l$ with $l \geq 2$. □

Lemma 6.1.5. *Let* $n > k$ *and* $k \leq 16$. *Then*

$$P(\Delta(n,k)) \leq 2k \tag{6.1.2}$$

implies that $(n,k) \in \{(8,2),(8,3)\}$ *or* $(n,k) \in [k+1,k]$ *for* $k \in \{2,3,5,6,8,9,11,14,15\}$ *or* $(n,k) \in [k+1,k,3]$ *for* $k \in \{4,7,10,13\}$ *or* $(n,k) \in [k+1,k,5]$ *for* $k \in \{12,16\}$.

Proof. We apply Lemma 6.1.1 to derive that (6.1.2) is possible only if $n = 3,8$ when $k = 2$ and $n = 5,6,7$ when $k = 4$. For the latter assertion, we apply Lemma 6.1.1 after securing $P((n+i)(n+j)) \leq 3$ with $0 \leq i < j \leq 3$ by deleting the terms divisible by 5 and 7 in $n, n+1, n+2$ and $n+3$. For $k = 3$ and $5 \leq k \leq 8$, the assertion follows from (1.2.3).

Thus we may assume that $k \geq 9$. Assume that (6.1.2) holds. Then there are at most $1 + [\frac{k-1}{p}]$ terms divisible by the prime p. After removing all the terms divisible by $p \geq 7$, we are left with at least 4 terms only divisible by $2, 3$ and 5. Further out of these terms, for each prime $2, 3$ and 5, we remove a term in which the prime divides to a maximal power. Then we are left with a term $n+i$ such that $n \leq n+i \leq 8 \times 9 \times 5 = 360$. Let $n \geq 2k$. We now apply Lemma 6.1.3 with $\mathfrak{N} = 361, k_0 = 9$ and (6.1.1) to get $P(\Delta(n,k)) > 2k$ for $k \geq 9$ except possibly when $p_i < n < n+k-1 < p_{i+1}$, $p_i = 113, 139, 181, 199, 211, 241, 283, 293, 317, 337$. For these values of n, we check that $P(\Delta(n,k)) > 2k$ is valid for $9 \leq k \leq 16$. Thus it suffices to consider $k < n < 2k$. We calculate $P(\Delta(n,k))$ for (n,k) with $9 \leq k \leq 16$ and $k < n < 2k$. We find that (6.1.2) holds only if (n,k) is given in the statement of the Lemma 6.1.5. □

Lemma 6.1.6. *Assume* (4.1.1) *and*

$$\mu \geq k - \pi(2k) + \pi(k). \tag{6.1.3}$$

Then we have

$$x < k^{\frac{3}{2}} \text{ for } k \geq 87;\ x < k^{\frac{7}{4}} \text{ for } k \geq 40;\ x < k^2 \text{ for } k \geq 19. \tag{6.1.4}$$

Lemma 6.1.7. *Let* $k \geq 57$. *Assume* (4.1.1), (6.1.3) *with* $x \geq 7k$. *Then* $x \geq k^{\frac{3}{2}}$.

The proofs of Lemmas 6.1.6, 6.1.7 are similar to that of Lemmas 4.2.5, 4.2.8, respectively.

6.2. Proof of Theorem 1.3.3 (a)

Let $n > \max(k+13, \frac{279}{262}k)$. In view of Lemma 6.1.5, we may take $k \geq 17$ since $n \leq k+5$ for the exceptions (n,k) given in Lemma 6.1.5. It suffices to prove (1.3.3) for k such that $2k-1$ is prime.

Let $k_1 < k_2$ be such that $2k_1 - 1$ and $2k_2 - 1$ are consecutive primes. Suppose (1.3.3) holds at k_1. Then for $k_1 < k < k_2$, we have

$$P(n(n+1)\cdots(n+k-1)) \geq P(n\cdots(n+k_1-1)) > 2k_1$$

implying $P(\Delta(n,k)) \geq 2k_2 - 1 > 2k$. Therefore we may suppose that $k \geq 19$ since $2k-1$ with $k = 17, 18$ are composites. We assume from now onward in the proof of Theorem 1.3.3 **(a)** that $2k-1$ is prime. We may suppose $\omega(\Delta(n,k)) \leq \pi(2k)$ otherwise (1.3.3) follows. We put $x = n+k-1$. Then $\Delta(n,k) = x(x-1)\cdots(x-k+1)$ and $\omega(x(x-1)\cdots(x-k+1)) \leq \pi(2k)$. Let $f_1 < f_2 < \cdots < f_\mu$ be all the integers in $[0,k)$ such that (4.1.1) holds. Then

$$\mu \geq k - \pi(2k) + \pi(k) \tag{6.2.1}$$

Now we apply Lemmas 6.1.6 and 6.1.7 to get $x < 7k$ for $k \geq 87$. Putting back $n = x - k + 1$ and using (6.1.4), we may assume that $n < 6k + 1$ for $k \geq 87$, $n < k^{\frac{7}{4}} - k + 1$ for $40 \leq k < 87$ and $n < k^2 - k + 1$ for $19 \leq k < 40$.

Let $k < 87$. Suppose $n \geq 2k$. Then $2k \leq n < k^{\frac{7}{4}} - k + 1$ for $40 \leq k < 87$ and $2k \leq n < k^2 - k + 1$ for $19 \leq k < 40$. Thus Lemma 6.1.3 with $\mathfrak{N} = 87^{\frac{7}{4}} - 87 + 1, k_0 = 35$ and (6.1.1) implies that $P(\Delta(n,k)) > 2k$ for $k \geq 35$. We note here that $2k \leq n < \mathfrak{N}$ for $35 \leq k < 40$. Let $k < 35$. Taking $\mathfrak{N} = 34^2 - 34 + 1, k_0 = 21$ for $21 \leq k \leq 34$ and $\mathfrak{N} = 19^2 - 19 + 1, k_0 = 19$ for $k = 19$, we see from Lemma 6.1.3 and (6.1.1) that $P(\Delta(n,k)) > 2k$ for $k \geq 19$. Here the case $k = 20$ is excluded since $2k-1$ is composite. Therefore we may assume that $n < 2k$. Further we observe that $\pi(n+k-1) - \pi(2k) \geq \pi(2k+13) - \pi(2k)$ since $n > k+13$. Next we check that $\pi(2k+13) - \pi(2k) > 0$. This implies that $[2k, n+k-1]$ contains a prime.

Thus we may assume that $k \geq 87$. Then we write $n = \alpha k + 1$ with $\frac{279}{262} - \frac{1}{k} < \alpha \leq 6$ if $k \geq 201$ and $1 + \frac{12}{k} < \alpha \leq 6$ if $k < 201$. Further we consider $\pi(n+k-1) - \pi(\max(n-1, 2k))$ which is

$$\begin{aligned} &= \pi((\alpha+1)k) - \pi(\alpha k) \quad \text{for } \alpha \geq 2 \\ &\geq \pi([\frac{541}{262}k]) - \pi(2k) \qquad \text{for } \alpha < 2 \text{ and } k \geq 201 \\ &\geq \pi(2k+13) - \pi(2k) \quad \text{for } \alpha < 2 \text{ and } k < 201. \end{aligned}$$

We check by using exact values of π function that $\pi(2k+13) - \pi(2k) > 0$ for $k < 201$ and $\pi([\frac{541}{262}k]) - \pi(2k) > 0$ for $201 \leq k \leq 2616$. Thus we may suppose that $k > 2616$ if $\alpha < 2$. Also $[\frac{541}{262}k] \geq \frac{540}{262}k$ for $k > 2616$. Now we apply Lemma 6.1.4 with $X = \alpha k, \theta = \frac{1}{\alpha}, l = 0$ if $\alpha \geq 2$ and $X = 2k, \theta = \frac{4}{131}, l = 1$ if $\alpha < 2$ to get $\pi(n+k-1) - \pi(\max(n-1, 2k)) > 0$ for $X > X_0 = \frac{5393}{1+\frac{1}{\alpha}}$ if $\alpha \geq 2$ and $X > X_1 = \frac{5393}{1+\frac{4}{131}}$ if $\alpha < 2$. Further when $\alpha < 2$, we observe that $X = 2k > X_1$ since $k > 2616$. Thus the assertion follows for $n < 2k$. It remains to consider the case $\alpha \geq 2$ and $X \leq 5393(1 + \frac{1}{\alpha})^{-1}$. Then $2k \leq n < n + k - 1 = X(1 + \frac{1}{\alpha}) \leq 5393$. Now we apply Lemma 6.1.3 with $\mathfrak{N} = 5393, k_0 = 35$ and (6.1.1) to conclude that $P(\Delta(n,k)) > 2k$. □

6.3. Proof of Theorem 1.3.3 (b)

In view of Lemma 6.1.5 and Theorem 1.3.3 **(a)**, we may assume that $k \geq 17$ and $k < n \leq \frac{279}{262}k$. Let $X = \frac{279}{262}k, \theta = \frac{245}{279}, l = 0$. Then for $k < n \leq X$, we see from Lemma 6.1.4 that

$$\pi(2k) - \pi(n-1) \geq \pi((1+\theta)X) - \pi(X) > 0$$

for $X > X_0 = 5393(1+\theta)^{-1}$ which is satisfied for $k > 2696$ since $(1+\theta)X = 2k$. Thus we may suppose that $k \leq 2696$. Now we check with exact values of π function that $\pi(2k) - \pi(\frac{279}{262}k) > 0$. Therefore $P(\Delta(n,k)) \geq P(n(n+1)\cdots 2k) \geq p_{\pi(2k)}$. Further we apply Lemma 6.1.4 with $X = 1.97k$, $\theta = \frac{3}{197}$ and $l = 25$. We calculate that $X_l \leq 284000$. We conclude by Lemma 6.1.4 that

$$\pi(2k) - \pi(1.97k) = \pi((1+\theta)X) - \pi(X) > 0$$

for $k > 145000$. Let $k \leq 145000$. Then we check that $\pi(2k) - \pi(1.97k) > 0$ is valid for $k \geq 680$ by using the exact values of π function. Thus

$$p_{\pi(2k)} > 1.97k \text{ for } k \geq 680. \tag{6.3.1}$$

Therefore we may suppose that $k < 680$. Now we observe that for $n > k+13$, $\pi(n+k-1)-\pi(1.97k) \geq \pi(2k+13) - \pi(1.97k) > 0$, the latter inequality can be checked by using exact values of π function. Hence the assertion follows since $n < 1.97k$. □

6.4. Proof of Theorem 1.3.1

By Theorem 1.3.3 (b), we may assume that $n \leq k+13$. Also we may suppose that $k < 680$ by (6.3.1). For $k \leq 16$, we calculate $P(\Delta(n,k))$ for all the pairs (n,k) given in the statement of Lemma 6.1.5. We find that either $P(\Delta(n,k)) > 1.95k$ or (n,k) is an exception stated in Theorem 1.3.3 (a). Thus we may suppose that $k \geq 17$. Now we check that $\pi(n+k-1) - \pi(1.95k) > 0$ except for $(n,k) \in [k+1, k, h]$ for $k \in A_h$ with $1 \leq h \leq 11$ and the assertion follows. □

6.5. Proof of Corollary 1.3.2

We calculate $P(\Delta(n,k))$ for all (n,k) with $k \leq 270$ and $k+1 \leq n \leq k+11$. This contains the set of exceptions given in Theorem 1.3.1. We find that $P(\Delta(n,k)) > 1.8k$ unless $(n,k) \in E_0$. Hence the assertion (1.3.2) follows from Theorem 1.3.1. □

CHAPTER 7

Refinement of an analogue of Sylvester's theorem for arithmetic progressions: Proof of Theorem 1.4.1

In this chapter, we prove Theorem 1.4.1. The proof of Theorem 1.4.1 depends on the sharpening of the upper bound for $\mathfrak{P}$ in the fundamental inequality of Sylvester and Erdős, see Lemma 7.1.1. Further we also give a better lower bound for $\mathfrak{P}$, see (7.3.12). Comparing the upper and lower bounds for $\mathfrak{P}$, we bound n, d and k. For the finitely many values of n, d, k thus obtained, we check the validity of (1.4.11) on a computer. When $d \leq 7$, we also need to use estimates on primes in arithmetic progression given in Lemma 3.1.5. We apply these estimates to count the number of terms of Δ which are of the form ap where $1 \leq a < d$, $\gcd(a, d) = 1$ and $p > k$, see Lemma 7.2.3.

7.1. Refinement of fundamental inequality of Sylvester and Erdős

For $0 \leq i < k$, let

$$n + id = B_i B_i' \tag{7.1.1}$$

where B_i and B_i' are positive integers such that $P(B_i) \leq k$ and $\gcd(B_i', \prod_{p \leq k} p) = 1$. Let $\mathcal{S} \subset \{B_0, \cdots, B_{k-1}\}$. Let $p \leq k$ be such that $p \nmid d$ and p divides at least one element of $\mathcal{S}$. Choose $B_{i_p} \in \mathcal{S}$ such that p does not appear to a higher power in the factorisation of any other element of $\mathcal{S}$. Let $\mathcal{S}_1$ be the subset of $\mathcal{S}$ obtained by deleting from $\mathcal{S}$ all such B_{i_p}. Let $\mathfrak{P}$ be the product of all the elements of $\mathcal{S}_1$.

The following lemma gives an upper bound for $\mathfrak{P}$ which is in fact a refinement of fundamental inequality of Sylvester and Erdős.

LEMMA 7.1.1. *Let $\mathcal{S}, \mathcal{S}_1, \mathfrak{P}$ be as above and let a' be the number of terms in $\mathcal{S}_1$ divisible by* 2. *Also we denote*

$$n_0 = \gcd(n, k-1)$$

and

$$\theta = \begin{cases} 1 \text{ if } 2 | n_0 \\ 0 \text{ otherwise.} \end{cases} \tag{7.1.2}$$

Then

$$\mathfrak{P} \leq n_0 \prod_{p \nmid d} p^{\mathrm{ord}_p((k-2)!)}. \tag{7.1.3}$$

Further for d odd, we have

$$\mathfrak{P} \leq 2^{-\theta} n_0 2^{a' + \mathrm{ord}_2([\frac{k-2}{2}]!)} \prod_{p \nmid 2d} p^{\mathrm{ord}_p((k-2)!)}. \tag{7.1.4}$$

PROOF. Let $p < k$, $p \nmid d$ be such that p divides at least one element of $\mathcal{S}$. Let $r_p \geq 0$ be the smallest integer such that $p \mid n + r_p d$. Write $n + r_p d = p n_1$. Then

$$n + r_p d, n + r_p d + pd, \cdots, n + r_p d + p[\frac{k-1-r_p}{p}]d$$

are all the terms in Δ divisible by p. Let $B_{r_p + p i_p}$ be such that p does not divide any other term of $\mathcal{S}$ to a higher power. Let a_p be the number of terms in $\mathcal{S}_1$ divisible by p. We note here that

$a_p \leq [\frac{k-1-r_p}{p}]$. For any $B_{r_p+pi} \in \mathcal{S}_1$, we have $\mathrm{ord}_p(B_{r_p+pi})$ $=\mathrm{ord}_p(n+r_pd+pid)$ $\leq \mathrm{ord}_p((n+r_pd+pid))-(n+r_pd+pi_pd))=1+\mathrm{ord}_p(i-i_p)$. Therefore

$$\mathrm{ord}_p(\mathfrak{P}) \leq a_p + \mathrm{ord}_p\left(\prod_{\substack{i=0\\ i\neq i_p}}^{[\frac{k-1-r_p}{p}]}(i-i_p)\right) \leq a_p + \mathrm{ord}_p\left(i_p![\frac{k-1-r_p}{p}-i_p]!\right) \tag{7.1.5}$$

Thus

$$\mathrm{ord}_p(\mathfrak{P}) \leq a_p + \mathrm{ord}_p([\frac{k-1-r_p}{p}]!). \tag{7.1.6}$$

Let $p \nmid n$. Then $r_p \geq 1$ and hence $a_p \leq [\frac{k-2}{p}]$. From (7.1.6), we have

$$\mathrm{ord}_p(\mathfrak{P}) \leq [\frac{k-2}{p}] + \mathrm{ord}_p([\frac{k-2}{p}]!) = \mathrm{ord}_p((k-2)!). \tag{7.1.7}$$

Let $p=2$. Then $a_2 = a'$ so that

$$\mathrm{ord}_2(\mathfrak{P}) \leq a' + \mathrm{ord}_2([\frac{k-2}{2}]!). \tag{7.1.8}$$

Let $p|n$. Then $r_p = 0$. Assume that $p \nmid (k-1)$. Then from (7.1.6), we have

$$\mathrm{ord}_p(\mathfrak{P}) \leq a_p + \mathrm{ord}_p([\frac{k-2}{p}]!). \tag{7.1.9}$$

Assume $p|(k-1)$ and let $i_0 \in \{0, \frac{k-1}{p}\}$ with $i_0 \neq i_p$ be such that $\mathrm{ord}_p(n+pi_0d)$ $=\min\,(\mathrm{ord}_p(n),\mathrm{ord}_p(k-1))$. If $\mathrm{ord}_p(n)$ $=\mathrm{ord}_p(k-1)$, we take $i_0 = 0$ if $i_p \neq 0$ and $i_0 = \frac{k-1}{p}$ otherwise. From (7.1.5), we have

$$\mathrm{ord}_p(\mathfrak{P}) \leq \min(\mathrm{ord}_p(n), \mathrm{ord}_p(k-1)) + a_p - 1 + \mathrm{ord}_p\left(\prod_{\substack{i=0\\ i\neq i_0, i_p}}^{\frac{k-1}{p}}(i-i_p)\right).$$

Thus

$$\mathrm{ord}_p(\mathfrak{P}) \leq \min(\mathrm{ord}_p(n), \mathrm{ord}_p(k-1)) + a_p - 1 + \mathrm{ord}_p((\frac{k-1-p}{p})!). \tag{7.1.10}$$

From (7.1.9) and (7.1.10), we conclude

$$\mathrm{ord}_p(\mathfrak{P}) \leq \min(\mathrm{ord}_p(n), \mathrm{ord}_p(k-1)) + [\frac{k-2}{p}] + \mathrm{ord}_p([\frac{k-2}{p}]!)$$

since $a_p \leq [\frac{k-1}{p}]$. Thus

$$\mathrm{ord}_p(\mathfrak{P}) \leq \min(\mathrm{ord}_p(n), \mathrm{ord}_p(k-1)) + \mathrm{ord}_p((k-2)!). \tag{7.1.11}$$

Now (7.1.3) follows from (7.1.7) and (7.1.11). Let $p=2$. By (7.1.9) and (7.1.10), we have in case of even n that

$$\mathrm{ord}_2(\mathfrak{P}) \leq \min(\mathrm{ord}_2(n), \mathrm{ord}_2(k-1)) - \theta + a' + \mathrm{ord}_2([\frac{k-2}{2}]!)$$

which, together with (7.1.7), (7.1.8) and (7.1.11), implies (7.1.8). □

The following Lemma is a consequence of Lemma 7.1.1.

Lemma 7.1.2. *Let $\alpha \geq 0$ and $m \geq 0$. Suppose $W(\Delta) \leq m$. Then there exists a set $\mathfrak{T} = \{n+i_hd | 0 \leq h \leq t,\ i_0 < i_1 < \cdots < i_t\}$ such that $1+t := |\mathfrak{T}| \geq k-m-\pi_d(k)$ satisfying*

$$d^t \leq \frac{n_0}{n}\frac{\prod_{p\nmid d} p^{\mathrm{ord}_p((k-2)!)}}{(\alpha+i_1)\cdots(\alpha+i_t)} \quad \text{if} \quad n = \alpha d \tag{7.1.12}$$

and

$$\frac{(n+i_0d)\cdots(n+i_td)}{2^a} \leq 2^{-\theta} n_0 2^{\mathrm{ord}_2([\frac{k-2}{2}]!)} \prod_{p\nmid 2d} p^{\mathrm{ord}_p((k-2)!)} \text{ if } d \text{ is odd} \tag{7.1.13}$$

where a is the number of even elements in $\mathfrak{T}$.

Proof. Let $\alpha > 0$ be given by $n = \alpha d$. Let $\mathfrak{S}$ be the set of all terms of Δ composed of primes not exceeding k. Then $|\mathfrak{S}| \geq k - m$. For every p dividing an element of $\mathfrak{S}$, we delete an $f(p) \in \mathfrak{S}$ such that

$$\mathrm{ord}_p(f(p)) = \max_{s\in\mathfrak{S}} \mathrm{ord}_p(s).$$

Then we are left with a set $\mathfrak{T}$ with $1 + t := |\mathfrak{T}| \geq k - m - \pi_d(k)$ elements of $\mathfrak{S}$. Let

$$\mathcal{P} := \prod_{\nu=0}^{t}(n+id) \geq (n+i_0d)(\alpha+i_1)\cdots(\alpha+i_t)d^t.$$

We now apply Lemma 7.1.1 with $\mathcal{S} = \mathfrak{S}$ and $\mathcal{S}_1 = \mathfrak{T}$ so that $\mathfrak{P} = \mathcal{P}$. Thus the estimates (7.1.3) and (7.1.4) are valid for $\mathcal{P}$. Comparing the upper and lower bounds of $\mathcal{P}$, we have (7.1.12) and further (7.1.13) for d odd. □

7.2. Lemmas for the proof of Theorem 1.4.1 (contd.)

The following lemma is analogue of Lemma 4.2.2 (ii) for $d > 1$.

Lemma 7.2.1. *Let $k_1 < k_2$ be such that $2k_1 - 1$ and $2k_2 - 1$ are consecutive primes. Suppose* (1.4.11) *holds at k_1. Then it holds for all k with $k_1 \leq k < k_2$.*

Proof. Assume that (1.4.11) holds at k_1. Let k be as in the statement of the lemma. Then $\pi(2k_1) = \pi(2k)$. From $\Delta(n,d,k) = n(n+d)\cdots(n+(k_1-1)d)(n+k_1d)\cdots(n+(k-1)d)$, we have

$$W(\Delta(n,d,k)) \geq W(\Delta(n,d,k_1)) \geq \pi(2k_1) - \pi_d(k_1) - \rho \geq \pi(2k) - \pi_d(k) - \rho$$

since $\pi_d(k) \geq \pi_d(k_1)$. □

Lemma 7.2.2. *Let* $\max(n,d) \leq k$. *Let* $1 \leq r < k$ *with* $\gcd(r,d) = 1$ *be such that*

$$W(\Delta(r,d,k)) \geq \pi(2k) - \rho.$$

Then for each n with $r < n \leq k$ and $n \equiv r(\mathrm{mod}\ d)$, we have

$$W(\Delta(n,d,k)) \geq \pi(2k) - \rho.$$

Proof. For $r < n \leq k$, we write

$$\begin{aligned}\Delta(n,d,k) &= \frac{r(r+d)\cdots(r+(k-1)d)(r+kd)\cdots(n+(k-1)d)}{r(r+d)\cdots(n-d)}\\ &= \Delta(r,d,k)\frac{(r+kd)\cdots(n+(k-1)d)}{r(r+d)\cdots(n-d)}.\end{aligned}$$

We observe that $p \mid \Delta(n,d,k)$ for every prime $p > k$ dividing $\Delta(r,d,k)$. □

Lemma 7.2.3. *Let $d \leq k$. For each $1 \leq r < d$ with* $\gcd(r,d) = 1$, *let r' be such that $rr' \equiv$ $1(\mathrm{mod}\ d)$. Then*
(a) For a given n with $1 \leq n \leq k$, Theorem 1.2.1 holds if

$$\sum_{\substack{1\leq r<d\\ \gcd(r,d)=1}} \pi\left(\frac{n+(k-1)d}{r}, d, nr'\right) - \pi(2k) + \rho \geq 0 \tag{7.2.1}$$

is valid.

(b) *For a given n with $k < n < 1.5k$, Theorem 1.2.1 holds if*

$$\sum_{\substack{1\le r<d\\ \gcd(r,d)=1}} \pi\left(\frac{k(d+1)-d+1}{r}, d, nr'\right) - \pi(2k) + \pi(k,d,n) - \pi(1.5k,d,n) \ge 0 \tag{7.2.2}$$

is valid.

(c) *For a given n with $k < n \le 2k$, Theorem 1.2.1 holds if*

$$\sum_{\substack{1\le r<d\\ \gcd(r,d)=1}} \pi\left(\frac{k(d+1)-d+1}{r}, d, nr'\right) - \pi(2k) + \pi(k,d,n) - \pi(2k,d,n) \ge 0 \tag{7.2.3}$$

is valid.

Proof. Let $1 \le r < d \le k$, $\gcd(r,d) = 1$. Then for each prime $p \equiv nr'(\text{mod } d)$ with $\max(k, \frac{n-1}{r}) < p \le \frac{n+(k-1)d}{r}$, there is a term $rp = n + id$ in $\Delta(n,d,k)$. Therefore

$$W(\Delta(n,d,k)) \ge \sum_{\substack{1\le r<d\\ \gcd(r,d)=1}} \left(\pi\left(\frac{n+(k-1)d}{r}, d, nr'\right) - \pi(\max(k, \frac{n-1}{r}), d, nr')\right). \tag{7.2.4}$$

Since

$$\sum_{\substack{1\le r<d\\ \gcd(r,d)=1}} \pi(k,d,nr') = \pi_d(k), \tag{7.2.5}$$

it is enough to prove (7.2.1) for deriving (1.4.11) for $1 \le n \le k$. This gives (a).

Let $k < n < k^{'}$ where $k^{'} = 1.5k$ or $2k+1$. Then from (7.2.4) and (7.2.5), we have

$$\begin{aligned} W(\Delta(n,d,k)) &\ge \sum_{\substack{1\le r<d\\ \gcd(r,d)=1}} \left(\pi\left(\frac{k+1+(k-1)d}{r}, d, nr'\right) - \pi(\max(k, \frac{k^{'}-1}{r}), d, nr')\right) \\ &\ge \sum_{\substack{1\le r<d\\ \gcd(r,d)=1}} \pi\left(\frac{k(d+1)-d+1}{r}, d, nr'\right) - \pi(k^{'}-1,d,n) - \pi_d(k) + \pi(k,d,n) \end{aligned}$$

since $r' = 1$ for $r = 1$. Hence it suffices to show (7.2.2) for proving (1.4.11) for $k < n < 1.5k$ or (7.2.3) for proving (1.4.11) for $k < n \le 2k$. Hence (b) and (c) are valid. □

7.3. Proof of Theorem 1.4.1 for k with $2k-1$ prime

Let

$$\chi = \chi(n) = \begin{cases} \min\left(1, \frac{k-1}{n}\prod\limits_{p|2d} p^{-\text{ord}_p(k-1)}\right) & \text{if } 2\nmid n \\ \min\left(2^{\theta-1}, \frac{k-1}{n}\prod\limits_{p|d} p^{-\text{ord}_p(k-1)}\right) & \text{if } 2\mid n \end{cases} \tag{7.3.1}$$

and

$$\chi_1 = \chi_1(n) = \min\left\{1, \frac{k-1}{n}\prod_{p|d} p^{-\text{ord}_p(k-1)}\right\}. \tag{7.3.2}$$

We observe that χ is non increasing function of n even and n odd separately. Further χ_1 is a non increasing function of n. We also check that

$$\frac{n_0}{n} \le \chi \le \chi_1 \tag{7.3.3}$$

and $\chi(1) = 1$, $\chi(2) = 2^{\theta-1}$.

We take $(n,d,k) \notin V$, $n > k$ when $d = 2$ so that $\rho = 0$. We assume that (1.4.11) is not valid and we shall arrive at a contradiction. We take $m = \pi(2k) - \pi_d(k) - 1$ in Lemma 7.1.2. Then $t \geq k - \pi(2k)$ in Lemma 7.1.2 and we have from (7.1.12) and (7.3.3) that

$$d^{k-\pi(2k)} \leq \chi_1(n) \frac{(k-2)! \prod_{p|d} p^{-\mathrm{ord}_p((k-2)!)}}{(\alpha+1)\cdots(\alpha+k-\pi(2k))} \tag{7.3.4}$$

where $n = \alpha d$ which is also the same as

$$\prod_{i=1}^{k-\pi(2k)} (n+id) \leq \chi_1(n)(k-2)! \prod_{p|d} p^{-\mathrm{ord}_p((k-2)!)}. \tag{7.3.5}$$

From (7.3.4), we have

$$d^{k-\pi(2k)} \leq \begin{cases} \chi_1(\alpha d)[\alpha]!(k-2)\cdots([\alpha]+k-\pi(2k)+1)\prod_{p|d} p^{-\mathrm{ord}_p(k-2)!} \text{ if } [\alpha] \leq \pi(2k)-3, \\ \chi_1(\alpha d)[\alpha]!\prod_{p|d} p^{-\mathrm{ord}_p(k-2)!} \text{ if } [\alpha] = \pi(2k)-2, \\ \chi_1(\alpha d)\frac{[\alpha]!}{(k-1)k(k+1)\cdots([\alpha]+k-\pi(2k))}\prod_{p|d} p^{-\mathrm{ord}_p(k-2)!} \text{ if } [\alpha] \geq \pi(2k)-1. \end{cases} \tag{7.3.6}$$

We observe that the right hand sides of (7.3.4), (7.3.5) and (7.3.6) are non-increasing functions of $n = \alpha d$ when d and k are fixed. Thus (7.3.6) and hence (7.3.4) and (7.3.5) are not valid for $n \geq n_0$ whenever it is not valid at $n_0 = \alpha_0 d$ for given d and k. This will be used without reference throughout this chapter. We obtain from (7.3.4) and $\chi_1 \leq 1$ that

$$d^{k-\pi(2k)} \leq (k-2)\cdots(k-\pi(2k)+1)\prod_{p|d} p^{-\mathrm{ord}_p(k-2)!} \tag{7.3.7}$$

which implies that

$$d^{k-\pi(2k)} \leq \begin{cases} (k-2)\cdots(k-\pi(2k)+1)2^{-\mathrm{ord}_2(k-2)!} \text{ if } d \text{ is even}, \\ (k-2)\cdots(k-\pi(2k)+1) \text{ if } d \text{ is odd} \end{cases} \tag{7.3.8}$$

and

$$d \leq (k-2)^{\frac{\pi(2k)-2}{k-\pi(2k)}} \prod_{p|d} p^{\frac{-\mathrm{ord}_p(k-2)!}{k-\pi(2k)}}. \tag{7.3.9}$$

Using Lemmas 3.1.2 (i) and 3.1.6, we derive from (7.3.9) that

(7.3.10)

$$d \leq \exp\left[\frac{\frac{2\log(k-2)}{\log 2k}(1+\frac{1.2762}{\log 2k}) - \frac{2\log(k-2)}{k}}{1-\frac{2}{\log 2k}(1+\frac{1.2762}{\log 2k})}\right] \prod_{p|d} p^{-\max\{0,(\frac{k-1-p}{p-1}-\frac{\log(k-2)}{\log p})/(k-\frac{2k}{\log 2k}(1+\frac{1.2762}{\log 2k}))\}}$$

which implies

$$d \leq \begin{cases} \exp\left[\frac{\frac{2\log(k-2)}{\log 2k}(1+\frac{1.2762}{\log 2k})-\frac{2\log(k-2)}{k}-\left((1-\frac{3}{k})\log 2-\frac{\log(k-2)}{k}\right)}{1-\frac{2}{\log 2k}(1+\frac{1.2762}{\log 2k})}\right] \text{ for } d \text{ even}, \\ \exp\left[\frac{\frac{2\log(k-2)}{\log 2k}(1+\frac{1.2762}{\log 2k})-\frac{2\log(k-2)}{k}}{1-\frac{2}{\log 2k}(1+\frac{1.2762}{\log 2k})}\right] \text{ for } d \text{ odd}. \end{cases} \tag{7.3.11}$$

We use the inequalities (7.3.5)-(7.3.11) at several places.

Let d be odd. Then for n even, $2 \mid n+id$ if and only if i is even and for n odd, $2 \mid n+id$ if and only if i is odd. Let $b = k-\pi(2k)+1-a$ and $a_0 = \min(k-\pi(2k)+1, [\frac{k-2+\theta}{2}])$. We note here that $a \leq [\frac{k-2+\theta}{2}]$ where θ is given by (7.1.2). Let n_e, d_e, n_o and d_o be positive integers with n_e even and

n_o odd. Let $n \geq n_e$ and $d \leq d_e$ for n even, and $n \geq n_o$ and $d \leq d_o$ for n odd. Assume (7.1.13). The left hand side of (7.1.13) is greater than

$$\begin{cases} \frac{n}{2} d^{k-\pi(2k)} \prod_{i=1}^{a-1} \left(\frac{n_e}{2d_e} + i\right) \prod_{j=1}^{b} \left(\frac{n_e}{d_e} + 2j - 1\right) := \dfrac{n}{2} d^{k-\pi(2k)} F(a) & \text{if } n \text{ is even} \\ n d^{k-\pi(2k)} \prod_{i=1}^{a} \left(\frac{n_o}{2d_o} + i - \frac{1}{2}\right) \prod_{j=1}^{b-1} \left(\frac{n_o}{d_o} + 2j\right) := n d^{k-\pi(2k)} G(a) & \text{if } n \text{ is odd.} \end{cases} \tag{7.3.12}$$

Let $A_e := \min\left(a_0, \left\lceil \frac{2}{3}(k - \pi(2k)) + \frac{n_e}{6d_e} + \frac{1}{3} \right\rceil\right)$ and $A_o := \min\left(a_0, \left\lceil \frac{2}{3}(k - \pi(2k)) + \frac{n_o}{6d_o} - \frac{1}{6} \right\rceil\right)$. By considering the ratios $\frac{F(a+1)}{F(a)}$ and $\frac{G(a+1)}{G(a)}$, we see that the functions $F(a)$ and $G(a)$ take minimal values at A_e and A_o, respectively. Thus (7.1.13) with (7.3.3) implies that

$$d^{k-\pi(2k)} F(A_e) \leq 2^{-\theta+1} \chi(n_e) 2^{\mathrm{ord}_2([\frac{k-2}{2}]!)} \prod_{p \nmid 2d} p^{\mathrm{ord}_p(k-2)!} \text{ for } n \text{ even} \tag{7.3.13}$$

since $\chi(n) \leq \chi(n_e)$ and

$$d^{k-\pi(2k)} G(A_o) \leq \chi(n_o) 2^{\mathrm{ord}_2([\frac{k-2}{2}]!)} \prod_{p \nmid 2d} p^{\mathrm{ord}_p((k-2)!)} \text{ for } n \text{ odd} \tag{7.3.14}$$

since $\chi(n) \leq \chi(n_o)$. In the following two lemmas, we bound d if (1.4.11) does not hold.

Lemma 7.3.1. *Let d be even. Assume that* (1.4.11) *does not hold. Then $d \leq 4$.*

Proof. Let d be even. By (7.3.11), $d \leq 6$ for $k \geq 860$. For $k < 860$, we use (7.3.8) to derive that

$$\begin{aligned} &d \leq 12 \text{ for } k \geq 9;\ d \leq 10 \text{ for } k = 100;\ d \leq 8 \text{ for } k > 57; \\ &d \leq 6 \text{ for } k > 255,\ k \neq 262, 310, 331, 332, 342. \end{aligned} \tag{7.3.15}$$

Let d be a multiple of 6. Then we see from (7.3.10) that $k \leq 100$. Again for $k \leq 100$, (7.3.7) does not hold. Let d be a multiple of 10. Then we see from (7.3.15) that $k = 100$ and $k \leq 57$. Again, (7.3.7) does not hold at these values of k.

Let $d = 8$. By (7.3.15), we may assume that $k \leq 255$ and $k = 262, 310, 331, 332, 342$. Let $n \leq k$. From Lemma 7.2.2, we need to consider only $n = 1, 3, 5, 7$ and (1.4.11) is valid for these values of n. Let $n = k + 1$. Then, we see that (7.3.5) does not hold. Thus (7.3.5) is not valid for all $n > k$. Hence $d \leq 4$. □

Lemma 7.3.2. *Let d be odd. Assume that* (1.4.11) *does not hold. Then $d \leq 53$ and d is prime.*

Proof. Let d be odd. We may assume that $d > 53$ whenever d is prime. Firstly we use (7.3.11) and then (7.3.8) to derive that $d \leq 15$ for $k \geq 2164$, $d \leq 59$ for $k \geq 9$ except at $k = 10, 12$, and $d \leq 141$ for $k = 10, 12$.

We further bring down the values of d and k by using (7.3.13) and (7.3.14). We shall be using (7.3.13) with $n_e = 2, \chi(n_e) = 2^{\theta-1}$ and (7.3.14) with $n_o = 1, \chi(n_o) = 1$ unless otherwise specified. Let $k < 2164$. We take $d_e = d_o = 59$ when $k \neq 10, 12$ and $d_e = d_o = 141$ for $k = 10, 12$. Let n be even. From (7.3.13), we derive that

$$\begin{aligned} &d \leq 27 \text{ for } k \geq 9, k \neq 10, 12, 16, 22, 24, 31, 37, 40, 42, 54, 55, 57; \\ &d \leq 57 \text{ for } k = 10, 12, 16, 22, 24, 31, 37, 40, 42, 54, 55, 57; \\ &d \leq 21 \text{ for } k > 100, k \neq 106, 117, 121, 136, 139, 141, 142, 147, 159; \\ &d \leq 17 \text{ for } k > 387, k \neq 415, 420, 432, 442, 444; \\ &d \leq 15 \text{ for } k > 957, k \neq 1072, 1077, 1081. \end{aligned} \tag{7.3.16}$$

Further we check that (7.3.16) holds for n odd using (7.3.14). Let $d > 3$ with $3 \mid d$. Then $k \leq 1600$ by (7.3.10) and $k \leq 850$ by (7.3.7). Further we apply (7.3.13) and (7.3.14) with $d_e = d_o = 57$ to conclude that $d = 9$, $k \leq 147$, $k = 157, 159, 232, 234$ and $d = 15$, $k = 10$. The latter case is excluded by applying (7.3.13) and (7.3.14) with $d_e = d_o = 15$. Let $d = 9$. Suppose $n \leq k$. We check that

(1.4.11) is valid for $1 \le n < 9$ and $\gcd(n,3)=1$. Now we apply Lemma 7.2.2 to find that (1.4.11) is valid for all $n \le k$. Let $n > k$. Taking $n_e = 2\lceil \frac{k+1}{2} \rceil, n_o = 2\lceil \frac{k}{2} \rceil + 1, d_e = d_o = 9$, we see that (7.3.13) and (7.3.14) are not valid for $n > k$.

Let $d > 15$ with $5 \mid d$ and $3 \nmid d$. Then $k \le 159$ by (7.3.16). Now, by taking $d_e = d_o = 55$, we see that (7.3.13) and (7.3.14) do not hold unless $k = 10, d = 25$ and n odd. We observe that (7.3.14) with $n_o = 3$ and $d_o = 25$ is not valid at $k = 10$. Thus $(n,d,k) = (1,25,10)$ and we check that (1.4.11) holds. Let $d > 7$ and $3 \nmid d, 5 \nmid d$. Then we see from (7.3.16) that $d = 49$ and $k = 10,12,16,22,24,31,37,40,42,54,55,57$. Taking $d_e = d_o = 49$, we see that both (7.3.13) and (7.3.14) do not hold. Thus $d < 57$ and the least prime divisor of d when $d \notin \{3,5,7\}$ is at least 11. Hence d is prime and $d \le 53$. □

In view of Lemmas 7.3.1 and 7.3.2, it suffices to consider $d = 2,4$ and primes $d \le 53$. We now consider some small values of d.

Lemma 7.3.3. *Let $d = 2,3,4,5$ and 7. Assume that $n \le k$ and $(n,d,k) \notin V$. Then* (1.4.11) *holds.*

Proof. First, we consider the case $1 \le n \le k$ and $(n,d,k) \notin V$. By Lemma 7.2.2, we may assume that $1 \le n < d$ and $\gcd(n,d) = 1$. Let $d = 2$. Then

$$\pi(n+2(k-1),2,1) - \pi(2k) + 1 = \pi(n+2k-2) - 1 - \pi(2k-1) + 1 \ge 0.$$

Now the assertion follows from Lemma 7.2.3. Let $d = 3,4,5$ or 7. We may assume that k is different from those given by $(n,d,k) \in V$, otherwise the assertion follows by direct computations. By using the bounds for $\pi(x,d,l)$ and $\pi(x)$ from Lemmas 3.1.5 and 3.1.2, we see that the left hand side of (7.2.1) is at least

$$(7.3.17) \qquad k\left\{\sum_{i=1}^{d-1} \frac{(\frac{d}{i} - \frac{d-1}{ik})}{\log \frac{1+dk-d}{i}} \left(\mathfrak{c}_1 + \frac{\mathfrak{c}_2}{\log \frac{1+dk-d}{2i}}\right) - \frac{2}{\log 2k}\left(1 + \frac{1.2762}{\log 2k}\right)\right\}$$

for $k \ge \frac{d-1}{d}(1+x_0)$ at $d = 3,5,7$ and

$$(7.3.18) \qquad k\left\{\sum_{i=1,3} \frac{(\frac{4}{i} - \frac{3}{ik})}{\log \frac{4k-3}{i}} \left(\mathfrak{c}_1 + \frac{\mathfrak{c}_2}{\log \frac{4k-3}{2i}}\right) - \frac{2}{\log 2k}\left(1 + \frac{1.2762}{\log 2k}\right)\right\}$$

for $k \ge \frac{3}{4}(1+x_0)$ at $d = 4$. Here x_0 is as given in Lemma 3.1.5. We see that (7.3.17) and (7.3.18) are increasing functions of k and (7.3.17) is non negative at $k = 20000, 2200, 1500$ for $d = 3,5$ and 7, respectively, and (7.3.18) is non negative at $k = 751$. Therefore, by Lemma 7.2.3, we conclude that k is less than 20000, 751, 2200 and 1500 according as $d = 3,4,5$ and 7, respectively. Further we recall that $n < d$. For these values of n and k, we check directly that (1.4.11) is valid. □

Therefore, by Lemma 7.3.3, we conclude that $n > k$ when $d = 2,3,4,5$ and 7.

Lemma 7.3.4. *Let $d = 2,3,4,5$ and 7. Assume that $k < n \le 2k$ if $d \ne 2$ and $k < n < 1.5k$ if $d = 2$. Then* (1.4.11) *holds.*

Proof. Let $d = 2$ and $k < n < 1.5k$. By Lemma 7.2.3, it suffices to prove (7.2.2). By using the bounds for $\pi(k)$ from Lemma 3.1.2, we see that the left hand side of (7.2.2) is at least

$$k\left\{\frac{3}{\log 3k - 1} + \frac{1}{\log k - 1} - \frac{2}{\log 2k}\left(1 + \frac{1.2762}{\log 2k}\right) - \frac{1.5}{\log 1.5k}\left(1 + \frac{1.2762}{\log 1.5k}\right)\right\} - 1$$

for $k \ge 5393$ since $\pi(3k-1,2,1) = \pi(3k) - 1$. We see that the above expression is an increasing function of k and it is non negative at $k = 5393$. Thus (7.2.2) is valid for $k \ge 5393$. For $k < 5393$, we check using exact values of π function that (7.2.2) is valid except at $k = 9,10,12$. For these values of k, we check directly that (1.4.11) is valid since $k < n < 1.5k$.

Let $d = 3,4,5,7$ and $k < n \le 2k$. By Lemma 7.2.3, it suffices to prove (7.2.3). By using the bounds for $\pi(x,d,l), \pi(2x,d,l) - \pi(x,d,l)$ and $\pi(k)$ from Lemmas 3.1.5 and 3.1.2, respectively, we see that (7.2.3) is valid for $k \ge 20000, 4000, 2500, 1500$ at $d = 3,4,5$ and 7, respectively. Thus we need to consider only $k < 20000, 4000, 2500, 1500$ for $d = 3,4,5$ and 7, respectively. (The estimate

(2.4) in [**27**] should have been replaced by (3.1.4) but it is clear that this causes no problem). Taking $n_e = 2\lceil\frac{k+1}{2}\rceil, n_o = 2\lceil\frac{k}{2}\rceil + 1, d_e = d_o = d$ for $d = 3, 5, 7$ in (7.3.13) and (7.3.14), and $n = k + 1$ for $d = 4$ in (7.3.5), we see that

$$\begin{aligned}
&k \leq 3226 \text{ or } k = 3501, 3510, 3522 \text{ when } d = 3\\
&k \leq 12 \text{ or } k = 16, 22, 24, 31, 37, 40, 42, 52, 54, 55, 57, 100, 142 \text{ when } d = 4\\
&k \leq 901 \text{ or } k = 940 \text{ when } d = 5\\
&k \leq 342 \text{ when } d = 7.
\end{aligned}$$

For these values of k, we check that (1.4.11) holds whenever $k < n < 1.5k$. Hence we may assume that $n \geq 1.5k$. Taking $n_e = 2\lceil\frac{1.5k}{2}\rceil, n_o = 2\lceil\frac{1.5k-1}{2}\rceil + 1, d_e = d_o = d$ for $d = 3, 5, 7$ in (7.3.13) and (7.3.14), and $n = \lceil 1.5k\rceil$ for $d = 4$ in (7.3.5), we see that

$$\begin{aligned}
&k \in \{54, 55, 57\} \text{ when } d = 3\\
&k \in \{10, 22, 24, 40, 42, 54, 55, 57, 70, 99, 100, 142\} \text{ when } d = 5\\
&k \in \{10, 12, 24, 37, 40, 42, 54, 55, 57, 100\} \text{ when } d = 7.
\end{aligned}$$

For these values of k, we check directly that (1.4.11) holds for $1.5k \leq n \leq 2k$. □

LEMMA 7.3.5. *Let $d = 2, 3, 4, 5$ and 7. Assume $n > 2k$ if $d \neq 2$ and $n \geq 1.5k$ if $d = 2$. Then* (1.4.11) *holds.*

PROOF. Let $d = 2$ and $n \geq 1.5k$. Then we take $\alpha = \frac{1.5k}{2}$ so that $n \geq \alpha d$. Further we observe that $\alpha \geq \pi(2k) - 1$. Then we see from (7.3.6) and (7.3.2) that

$$2^{k-\pi(2k)} \leq \frac{\lceil .75k\rceil !}{1.5k^2(k+1)\cdots(\lceil .75k\rceil + k - \pi(2k))}\ 2^{-\mathrm{ord}_2(k-1)!}. \tag{7.3.19}$$

Now we apply Lemmas 3.1.7, 3.1.6 and 3.1.2 (i) in (7.3.19) to derive that

$$\begin{aligned}
2 &\leq \left(\frac{\frac{8}{3}\sqrt{2\pi}\ \exp(-.75k)(.75(k+1))^{.75(k+1)+\frac{1}{2}}\ \exp(\frac{1}{9k})2^{\pi(2k)}}{k^2(k+1)^{.75k-\pi(2k)}}\right)^{\frac{1}{2k-\frac{\log(k-1)}{\log 2}}}\\
&\leq \exp\left(\frac{\frac{2\log 2(k+1)}{\log 2k}(1+\frac{1.2762}{\log 2k}) - .75 + .75\log .75 + \frac{1}{9k^2} + \frac{1.25\log(k+1)-2\log k+1.54017}{k}}{2-\frac{\log(k-1)}{k\log 2}}\right)
\end{aligned}$$

for $k \geq 9$. This does not hold for $k \geq 700$. Thus $k < 700$. Further using (7.3.5) with $n = \lceil 1.5k\rceil$, we get $k \in \{16, 24, 54, 55, 57, 100, 142\}$. For these values of k, taking $n = 2k + 1$, we see that (7.3.5) is not valid. Thus $n \leq 2k$. Now we check that (1.4.11) holds for these values of k and $1.5 \leq n \leq 2k$.

Let $d = 3, 4, 5$ and 7 and $n > 2k$. Then we take $\alpha = \frac{2k+1}{d}$ so that $n \geq \alpha d$. We proceed as in the case $d = 2$ to derive from (7.3.5) that $k < 70, 69, 162$ and 1515 for $d = 3, 4, 5$ and 7, respectively. Let $d = 3, 5$ and 7. We use (7.3.13) and (7.3.14) with $n_e = 2k + 2, n_o = 2k + 1$ and $d_e = d_o = d$ if $d = 3, 5, 7$, respectively to get $d = 5, k = 10$ and n even. Let $k = 10, d = 5$ and n even. We take $n_e = 2k+6, d_e = 5$ to see that (7.3.13) holds. Hence $n \leq 2k+4$. Now we check directly that (1.4.11) is valid for $n = 2k + 2, 2k + 4$. Finally we consider $d = 4$ and $k < 69$. Taking $n = 2k + 1$, we see that (7.3.5) is not valid. Thus (1.4.11) holds for all $n > 2k$. □

By Lemmas 7.3.1, 7.3.2, 7.3.3, 7.3.4, and 7.3.5, it remains to consider

$$11 \leq d \leq 53, d \text{ prime}.$$

We prove Theorem 1.4.1 for these cases in the next section.

7.3.1. The Case d≥ 11 with d prime. Our strategy is as follows. Let $U_0, U_1, \cdots$ be sets of positive integers. For any two sets U and V, we denote $U - V = \{u \in U | u \notin V\}$. Let d be given. We take $d_e = d_o = d$ always unless otherwise specified. We apply steps $1 - 5$ as given below.

1. Let $d = 11, 13$. We first use (7.3.10) to bound k. We reduce this bound considerably using (7.3.7). For $d > 13$, we use (7.3.16) to bound k. Then we apply (7.3.13) and (7.3.14) with $n_e = n_e^{(0)} = 2, n_o = n_o^{(0)} = 1$ to bring down the values of k still further. Let U_0 be these finite set of values of k.
2. For each $k \in U_0$, we check that (1.4.11) is valid for $1 \leq n < d$. Hence by Lemma 7.2.2, we get $n > k$.
3. For $k \in U_0$, we apply (7.3.5) with $n = k + 1$ to find a subset $U_0^{'} \subsetneq U_0$.
4. For $k \in U_0^{'}$, we apply (7.3.13) and (7.3.14) with $n_e = n_e^{(1)} = 2\lceil \frac{k+1}{2} \rceil, n_o = n_o^{(1)} = 2\lceil \frac{k}{2} \rceil + 1$ to get a subset $U_1 \subsetneq U_0^{'}$.
5. Let $i \geq 2$. For $k \in U_{i-1}$, we apply (7.3.13) and (7.3.14) with suitable values of $n_e = n_e^{(i)}$ and $n_o = n_o^{(i)}$ to get a subset $U_i \subsetneq U_{i-1}$. Thus for $k \in U_{i-1} - U_i$, we have $k < n < \max(n_e^{(i)}, n_o^{(i)})$ and we check that (1.4.11) is valid for these values of n and k. We stop as soon as $U_i = \phi$.

We explain the above strategy for $d = 11$. From (7.3.10), we get $k \leq 11500$ which is reduced to $k \leq 5589$ by (7.3.7). By taking $n_e^{(0)} = 2, n_o^{(0)} = 1$, we get

$$U_0 = \{k | k \leq 2977, k = 3181, 3184, 3187, 3190, 3195, 3199\}.$$

We now check that (1.4.11) is valid for $1 \leq n < 11$ for each $k \in U_0$ so that we conclude $n > k$. By Step 3, we get $U_0^{'} = \{k | k \leq 252\}$. Further by step 4, we find

$$U_1 = \{9, 10, 12, 16, 21, 22, 24, 27, 31, 37, 40, 42, 45, 52, 54, 55, 57, 70, 91, 99, 100, 121, 142\}.$$

Now we take

$$n_e^{(2)} = 2\lceil \frac{1.5k}{2} \rceil, \ n_o^{(2)} = 2\lceil \frac{1.5k - 1}{2} \rceil + 1$$

to get $U_2 = \{10, 22, 37, 42, 54, 55, 57\}$. Then we have

$$k < n < 1.5k \text{ for } k \in U_1 - U_2. \tag{7.3.20}$$

Next we take $n_e^{(3)} = 2k + 2, n_o^{(3)} = 2k + 1$ to get $U_3 = \{10, 22, 55\}$ and we have

$$k < n < 2k \text{ for } k \in U_2 - U_3. \tag{7.3.21}$$

Finally we take $n_e^{(4)} = 4k, n_o^{(4)} = 4k + 1$ to get $U_4 = \phi$ and hence

$$k < n < 4k \text{ for } k \in U_3 \tag{7.3.22}$$

and our procedure stops here since $U_4 = \phi$. Now we check that (1.4.11) holds for k and n as given by (7.3.20), (7.3.21) and (7.3.22).

We follow steps $1 - 5$ with the same parameters as for $d = 11$ in the cases $d = 13, 17, 19$ and 23. Let $23 < d \leq 53$, d prime. We modify our steps $1 - 5$ slightly to cover all these values of d simultaneously. For each of $k \in U_0$, we check that (1.4.11) is valid for $1 \leq n \leq \min(d, k)$ and coprime to d. Thus $n > k$. Now we apply step 4 with $d_e = d_o = 53$ to get $U_1 = \{10, 12, 16, 24, 37, 55, 57\}$. In step 5, we take $n_e^{(2)} = 2\lceil \frac{3k+1}{2} \rceil, n_o^{(2)} = 2\lceil \frac{3k}{2} \rceil + 1, d_e = d_o = 53$ to see that that $U_2 = \phi$. Thus

$$k < n < 3k \text{ for } k \in U_1. \tag{7.3.23}$$

Now we check that (1.4.11) holds for k and n as given by (7.3.23) for every d with $23 < d \leq 53$ and d prime. □

7.4. Proof of Theorem 1.4.1

By the preceding section, Theorem 1.4.1 is valid for all k such that $2k - 1$ is prime. Let k be any integer and $k_1 < k < k_2$ be such that $2k_1 - 1, 2k_2 - 1$ are consecutive primes. By Lemma 7.2.3, we see that (1.4.11) is valid except possibly for those triples (n, d, k) with $(n, d, k_1) \in V$. We check the validity of (1.4.11) at those (n, d, k). For instance, let $k = 11$. Then $k_1 = 10$. We see that $(1, 3, 10), (4, 3, 10), (2, 5, 10), (1, 7, 10) \in V$. We check that (1.4.11) does not hold at $(1, 3, 11)$ and (1.4.11) holds at $(4, 3, 11), (2, 5, 11)$ and $(1, 7, 11)$. Thus $(1, 3, 11) \in V$. We find that all the exceptions to Theorem 1.4.1 are given by V. □

7.5. Proof of (1.4.8)

Let $k = 8$ and (n, d) be different from the ones given by (1.4.9). Suppose (1.4.8) is not valid. Then

$$W(\Delta) \leq k - 2 - \pi_d(k). \tag{7.5.1}$$

We apply Lemma 7.1.2 with $m = k - 2 - \pi_d(k)$. We see from $t \geq 1$ and (7.1.12) that

$$n + d \leq \frac{n_0}{n} 6! \prod_{p|d} p^{-\mathrm{ord}_p(6!)}. \tag{7.5.2}$$

Since $n_0 = 7$ if $7|n$ and 1 otherwise, we observe that $1 + d \leq n + d \leq 6! \prod_{p|d} p^{-\mathrm{ord}_p(6!)}$. For instance, we get $n + d \leq 3 \cdot 15 = 15$ when $2|d$. For each d with $1 < d \leq 6! \prod_{p|d} p^{-\mathrm{ord}_p(6!)} - 1$ and for each n satisfying (7.5.2), we check that

$$|\{P(n + id) : 0 \leq i \leq 7\}| \geq 7$$

hold except when (n, d) is given by

$$\begin{gathered} d = 4,\ n = 21;\ d = 7,\ n \in \{3, 5, 6\}; \\ d = 11,\ n = 3;\ d = 17,\ n = 6; \\ d = 19,\ n = 5;\ d = 23,\ n = 1. \end{gathered} \tag{7.5.3}$$

Now we get a contradiction from (7.5.1) since (7.5.1) is not valid for (n, d) given by (7.5.3) and

$$W(\Delta) = |\{P(n + id) : 0 \leq i \leq 7\}| - |\{P(n + id) : P(n + id) \leq k, 0 \leq i \leq 7\}| \geq 7 - \pi_d(k)$$

for (n, d) different from (7.5.3). □

CHAPTER 8

Refinement of Sylvester's theorem on the greatest prime divisor of a product of terms of an arithmetic progression: Proof of Theorem 1.5.1

In this chapter, we prove Theorem 1.5.1. The proof of Theorem 1.5.1 depends on Theorem 1.4.1 and the theory of linear forms in logarithms. The cases $k = 3, 4, 5$ involve solving particular cases of Catalan's equation and Generalised Fermat's equation. The cases $6 \leq k \leq 11$ requires solving some Thue equations. For $12 \leq k \leq 18$, we get a bound for n and d by counting the number of terms in Δ divisible by a prime $\leq 2k$ and we check the assertion. When $k \geq 19$, we follow the arguments in the proof of Theorem 1.4.1 under certain assumptions which are valid in the present context.

8.1. Lemmas

We begin with

Lemma 8.1.1. *It suffices to prove Theorem 1.5.1 for k such that $2k - 1$ is prime.*

Proof. Let (n, d, k) be as in Theorem 1.5.1. Let k_1 and k_2 be such that $k_1 < k < k_2$ and $2k_1 - 1, 2k_2 - 1$ are consecutive primes. Assume that (1.5.2) holds at (n, d, k_1). Then

$$P(n(n + d) \cdots (n + (k - 1)d) \geq P(n \cdots (n + (k_1 - 1)d)) > 2k_1$$

implying $P(\Delta(n, d, k)) \geq 2k_2 - 1 > 2k$. Thus (1.5.2) holds at (n, d, k).

Therefore (1.5.2) is valid except possibly for those triples (n, d, k) with (n, d, k_1) as one of the exceptions in Theorem 1.5.1. We check the validity of (1.5.2) at those (n, d, k). For instance, let $k = 11$. Then $k_1 = 10$. We see that $(1, 3, 10)$ is the only exception in Theorem 1.5.1. We check that (1.5.2) holds at $(1, 3, 11)$. □

For a proof of the following result, we refer to de Weger [**80**, Theorem 5.2]. It is a particular case of Catalan equation which has been solved completely by Mihăilescu [**41**].

Lemma 8.1.2. *Let $a, b \in \{2, 3, 5\}$ and $a < b$. Then the solutions of*

$$a^x - b^y = \pm 1 \text{ in integers } x > 0, y > 0$$

are given by

$$(a^x, b^y) \in \{(2^2, 3), (2, 3), (2^3, 3^2), (2^2, 5)\}.$$

The next result is due to Nagell [**49**], see [**3**].

Lemma 8.1.3. *Let $a, b, c \in \{2, 3, 5\}$ and $a < b$. Then the solutions of*

$$a^x + b^y = c^z \text{ in integers } x > 0, y > 0, z > 0$$

are given by

$$\begin{aligned}(a^x, b^y, c^z) \in \{&(2, 3, 5), (2^4, 3^2, 5^2), (2, 5^2, 3^3),\\ &(2^2, 5, 3^2), (3, 5, 2^3), (3^3, 5, 2^5), (3, 5^3, 2^7)\}.\end{aligned}$$

We shall also need some more equations given by the following. See also de Weger [**80**, Theorem 5.5].

Lemma 8.1.4. *Let $\delta \in \{1, -1\}$. The solutions of*

$$\begin{aligned} &(i) \quad 2^x - 3^y 5^z = \delta \\ &(ii) \quad 3^x - 2^y 5^z = \delta \\ &(iii) \; 5^x - 2^y 3^z = \delta \end{aligned}$$

in integers $x > 0, y > 0, z > 0$ are given by

$$(x, y, z, \delta) = \begin{cases} (4,1,1,1) & \text{for } (i); \\ (4,4,1,1), (2,1,1,-1) & \text{for } (ii); \\ (2,3,1,1), (1,1,1,-1) & \text{for } (iii), \end{cases}$$

respectively.

Proof. (i) Let $\delta = 1$. By $2^x \equiv 1 (\text{mod } 5)$, we get $4|x$. This implies $2^{\frac{x}{2}} - 1 = 3^y, 2^{\frac{x}{2}} + 1 = 5^z$ and the assertion follows from Lemma 8.1.2. Let $\delta = -1$. Then $2^x \equiv -1(\text{mod } 5)$ and $2^x \equiv -1(\text{mod } 3)$ implying $2|x$ and $2 \nmid x$, respectively. This is a contradiction.

(ii) Let $\delta = 1$. By $3^x \equiv 1(\text{mod } 5)$ giving $4|x$ and the assertion follows as in (i) with $\delta = 1$. Let $\delta = -1$. Let $y \geq 2$. Then $3^x \equiv -1(\text{mod } 5)$ and $3^x \equiv -1(\text{mod } 4)$ implying $2|x$ and $2 \nmid x$, respectively. Therefore $y = 1$ and we rewrite equation (ii) as $2 \cdot 5^z - 3^x = 1$. We may assume that $z \geq 2$ and further x is even by reading mod 4. Thus $3^x \equiv -1(\text{mod } 25)$ giving $x \equiv 10(\text{mod } 20)$. Then $\frac{x}{10}$ is odd and

$$1 + 9^5 \text{ divides } 1 + (9^5)^{\frac{x}{10}} = 2 \cdot 5^z,$$

a contradiction.

(iii) Let $\delta = 1$. By mod 3, we get x even and the assertion follows as in (i) with $\delta = 1$. Let $\delta = -1$. We may assume that $y = 1$ by mod 4 and $z \geq 2$. Then we derive as in (ii) with $\delta = -1$ that $\frac{x}{3}$ is odd by using mod 9 and $1 + 5^3$ divides $1 + 5^x = 2 \cdot 3^z$, a contradiction. □

We write $p(d)$ for the least prime divisor of d. We shall use the following computational result.

Lemma 8.1.5. *Assume that $p(d) > k$ if $k = 6, 7$ and $p(d) > 2k$ if $k = 9, 10, 12, 15, 16$. Then* (1.5.2) *holds if*

$$n + d \leq N$$

where

$$N = \begin{cases} 20 \cdot 3^5 & \text{if } k = 6, 7, \\ 40 \cdot 3^6 & \text{if } k = 9, 10, \\ 360 & \text{if } = 12, 15, 16. \end{cases}$$

Proof. For each n with $1 \leq n \leq N$ and $P(n) \leq 2k$, we check the validity of $\max\{P(n + (k - 1)d), P(n + (k - 2)d), P(n + (k - 3)d)\} > 2k$ whenever $d \leq N - n$ and $p(d) > k$ if $k = 6, 7$ and $p(d) > 2k$ if $k \geq 9$. If $\max\{P(n+(k-1)d), P(n+(k-2)d), P(n+(k-3)d)\} \leq 2k$, then we check the validity of $\max\{P(n+d), P(n+2d)\} > 2k$. Then we find that either $\max\{P(n+d), P(n+2d)\} > 2k$ or

(8.1.1) $\quad (n, d) \in \{(33, 31), (64, 31)\}$ if $k = 12$ and $(n, d) \in \{(3, 31), (34, 31), (35, 43)\}$ if $k = 15$.

For (n, d, k) given by (8.1.1), we check that $P(\Delta(n, d, k)) > 2k$. □

Let $n \geq 1, d > 2$ and $k \geq 3$. By Lemma 8.1.1, we may restrict to those k for which $2k - 1$ is prime. For $(n, d, k) \in V_0 \cup V$ where V_0 and V are defined in (1.4.6) and (1.4.10), respectively, we check that $P(\Delta(n, d, k)) > 2k$. Therefore we assume that $(n, d, k) \notin V_0 \cup V$. If $p(d) \leq k$ for $k = 6, 7$ and $p(d) \leq 2k$ for $k \geq 9$, then the assertion follows from (1.4.5) and (1.4.12), respectively. Thus we may suppose that $p(d) > k$ for $k = 6, 7$ and $p(d) > 2k$ for $k \geq 9$. Therefore the assumption of Lemma 8.1.5 is satisfied. We shall follow the assumptions stated in this paragraph throughout this chapter. We split the proof of Theorem 1.5.1 for $k = 3$; $k = 4$; $k = 6, 7, 9, 10$; $k = 12, 15, 16$ and $k \geq 19$ with $2k - 1$ prime in sections 8.2, 8.3, 8.4, 8.5 and 8.6, respectively.

8.2. The case $k = 3$

We assume that $P(n(n+d)(n+2d)) \leq 5$ and (n,d) is different from the exceptions given in Theorem 1.5.1. Let $5 \nmid \Delta$. Then either

$$n = 1, 1 + d = 2^\alpha, 1 + 2d = 3^\beta \text{ or } n = 2, 2 + d = 3^\beta, 2 + 2d = 2^\alpha.$$

Assume the first possibility. Then $2^{\alpha+1} - 3^\beta = 1$ implying $2^{\alpha+1} = 4, 3^\beta = 3$ by Lemma 8.1.2. Thus $d = 1$, a contradiction. Now we turn to the second. We get $3^\beta - 2^{\alpha-1} = 1$. Therefore either $3^\beta = 2, 2^{\alpha-1} = 2$ or $3^\beta = 9, 2^{\alpha-1} = 8$ by Lemma 8.1.2. The former is not possible since $P2kd > 1$ and the latter implies that $d = 7$ which is excluded. Hence $5|\Delta$.

Suppose $3 \nmid \Delta$. We observe that $5 \nmid n$ since $\gcd(n+d, n+2d) = 1$. Let $5|n+2d$. Then $n = 1, 1+d = 2^\alpha, 1+2d = 5^\gamma$ implying $2^{\alpha+1} - 5^\gamma = 1$ which is not possible by Lemma 8.1.2. Let $5|n+d$. Then $n = 2^\eta, n+d = 5^\gamma, n+2d = 2^\alpha$ implying $n = 2, 5^\gamma - 2^{\alpha-1} = 1$. Therefore by Lemma 8.1.2, we get $n = 2, d = 3$ which is excluded. Hence $3|\Delta$.

Let $15|n+id$ for some $i \in \{0,1,2\}$. We observe that $15 \nmid n$ since $\gcd(n+d, n+2d) = 1$. Let $15|n+d$. Then $n = 2, 2+d = 3^\beta 5^\gamma, 2+2d = 2^\alpha$ giving $2^{\alpha-1} - 3^\beta 5^\gamma = -1$ which is not possible by Lemma 8.1.4 (i). Let $15|n+2d$. Then $n = 1, 1+d = 2^\alpha, 1+2d = 3^\beta 5^\gamma$ giving $2^{\alpha+1} - 3^\beta 5^\gamma = 1$. Therefore by Lemma 8.1.4 (i), we get $n = 1, d = 7$ which is excluded. Thus $15 \nmid n+id$ for $i = 0,1,2$.

Suppose $2 \nmid \Delta$. Then

$$n = 1, 1+d = 3^\beta, 1+2d = 5^\gamma \text{ or } n = 1, 1+d = 5^\gamma, 1+2d = 3^\beta$$

which imply $5^\gamma - 2 \cdot 3^\beta = -1$ or $3^\beta - 2 \cdot 5^\gamma = -1$, respectively. Therefore $(n,d) = (1,2)$ or $(1,4)$ by Lemma 8.1.4. This is not possible. Hence $2|\Delta$.

Let $n = 1$. In view of the above conclusions in this section, we have

$$1 + d = 2^\alpha 3^\beta, 1 + 2d = 5^\gamma \text{ or } 1 + d = 2^\alpha 5^\gamma, 1 + 2d = 3^\beta$$

implying $5^\gamma - 2^{\alpha+1} \cdot 3^\beta = -1$ or $3^\beta - 2^{\alpha+1} \cdot 5^\gamma = -1$, respectively, contradicting Lemma 8.1.4 since $\alpha \geq 1$. Let $n = 2$. Then $2 + d = 3^\beta, 2 + 2d = 2^\alpha 5^\gamma$ or $2 + d = 5^\gamma, 2 + 2d = 2^\alpha 3^\beta$ implying $3^\beta - 2^{\alpha-1} \cdot 5^\gamma = 1$ or $5^\gamma - 2^{\alpha-1} \cdot 3^\beta = 1$, respectively. By Lemma 8.1.4, the first equation gives $d = 79$ and the second one gives $d = 23$ which are excluded. Thus $n > 2$. Now we have

$$\begin{aligned}
&n = 2^\alpha, n+d = 3^\beta, n+2d = 2 \cdot 5^\gamma \quad \text{or} \quad n = 2^\alpha, n+d = 5^\gamma, n+2d = 2 \cdot 3^\beta \\
\text{or} \quad &n = 2 \cdot 3^\beta, n+d = 5^\gamma, n+2d = 2^\alpha \quad \text{or} \quad n = 2 \cdot 5^\gamma, n+d = 3^\beta, n+2d = 2^\alpha \\
\text{or} \quad &n = 3^\beta, n+d = 2^\alpha, n+2d = 5^\gamma \qquad \text{or} \quad n = 5^\gamma, n+d = 2^\alpha, n+2d = 3^\beta.
\end{aligned}$$

By using the identity

$$n + (n+2d) - 2(n+d) = 0, \tag{8.2.1}$$

we see that the above relations imply equations of the form given by Lemma 8.1.3. Now we use Lemma 8.1.3 to find all the pairs (n,d) arising out of the solutions of these equation. Finally we observe that these pairs (n,d) are already excluded. □

8.3. The case $k = 4$

We shall derive Theorem 1.5.1 with $k = 4$ from the case $k = 3$ and the following more general result. We put $\Delta_1 = n(n+2d)(n+3d)$ and $\Delta_2 = n(n+d)(n+3d)$. Let

$$S_{41} = \{(1,13), (3,11), (4,7), (6,7), (6,13), (18,119), (30,17)\}$$

and

$$\begin{aligned}
S_{42} = \{&(1,3), (1,5), (1,8), (1,53), (3,2), (3,5), (3,17), \\
&(3,29), (3,47), (9,7), (9,247), (15,49), (27,23)\}.
\end{aligned}$$

LEMMA 8.3.1. *We have*

$$P(\Delta_1) \geq 7 \text{ unless } (n,d) \in S_{41} \tag{8.3.1}$$

and

$$P(\Delta_2) \geq 7 \text{ unless } (n,d) \in S_{42}. \tag{8.3.2}$$

PROOF. First we prove (8.3.1). Assume that $(n,d) \notin S_{41}$ and $P(\Delta_1) \leq 5$. Suppose $5 \nmid \Delta_1$. Then either

$$n = 1, 1+2d = 3^\beta, 1+3d = 2^\alpha \text{ or } n = 6, 6+2d = 2^\alpha, 6+3d = 3^\beta.$$

This is not possible by Lemma 8.1.2 since $d > 1$. Suppose $3 \nmid \Delta_1$. Then either $n = 1, 1+2d = 5^\gamma, 1+3d = 2^\alpha$ or $n = 2, 2+2d = 2^\alpha, 2+3d = 5^\gamma$. This is again not possible by Lemma 8.1.4 (*i*), (*iii*). Suppose $2 \nmid \Delta_1$. Then either $n = 1, 1+2d = 3^\beta, 1+3d = 5^\gamma$ or $n = 3, 3+2d = 5^\gamma, 3+3d = 3^\beta$. This is not valid by Lemma 8.1.4 (*ii*), (*iii*). Hence $2 \cdot 3 \cdot 5 \mid \Delta_1$.

Let $n = 1$. Then either $1+2d = 3^\beta 5^\gamma, 1+3d = 2^\alpha$ or $1+2d = 3^\beta, 1+3d = 2^\alpha 5^\gamma$. The first possibility is excluded by Lemma 8.1.4 (*i*) and second possibility implies $d = 13$ by Lemma 8.1.4 (*ii*). Let $n = 2$. Then $2+2d = 2^\alpha 3^\beta, 2+3d = 5^\gamma$ which is not possible by Lemma 8.1.4 (*iii*). Let $n = 3$. Then $3+2d = 5^\gamma, 3+3d = 2^\alpha 3^\beta$ implying $d = 11$ by Lemma 8.1.4 (*iii*). Let $n = 6$. Then either $6+2d = 2^\alpha 5^\gamma, 6+3d = 3^\beta$ or $6+2d = 2^\alpha, 6+3d = 3^\beta 5^\gamma$. The first possibility implies $d = 7$ by Lemma 8.1.4 (*ii*) and second implies $d = 13$ by Lemma 8.1.4 (*i*).

Let $n = 4, 5$ or $n > 6$. We observe that $n = 2^{\delta_1} 5^\gamma$ with $\delta_1 \geq 1$ or $3^{\delta_2} 5^\gamma$ with $\delta_2 \geq 1$ are not possible since otherwise $P(n+3d) > 5$ or $P(n+2d) > 5$, respectively. Let $n = 2^{\delta_1} 3^{\delta_2}$ or $n = 2^{\delta_1} 3^{\delta_2} 5^\gamma$ with $\delta_1 \geq 1, \delta_2 \geq 1$. Then

$$\delta_1 = 1, n = 2 \cdot 3^\beta, n+2d = 2^\alpha, n+3d = 3 \cdot 5^\gamma$$
$$\text{or } \delta_2 = 1, n = 3 \cdot 2^\alpha, n+2d = 2 \cdot 5^\gamma, n+3d = 3^\beta.$$

if $n = 2^{\delta_1} 3^{\delta_2}$ and

$$\delta_1 = 1, \delta_2 = 1, n = 6 \cdot 5^\gamma, n+2d = 2^\alpha, n+3d = 3^\beta$$

if $n = 2^{\delta_1} 3^{\delta_2} 5^\gamma$. Further

$$n+2d = 2 \cdot 3^\beta, n+3d = 5^\gamma \text{ if } n = 2^\alpha$$
$$n+2d = 5^\gamma, n+3d = 3 \cdot 2^\alpha \text{ if } n = 3^\beta$$
$$n+2d = 3^\beta, n+3d = 2^\alpha \text{ if } n = 5^\gamma.$$

This exhaust all the possibilities. For each of the above relations, we use the identity

$$n + 2(n+3d) - 3(n+2d) = 0 \tag{8.3.3}$$

to obtain an equation of the form given by Lemma 8.1.3. Finally we apply Lemma 8.1.3 as in the preceding section to conclude that $(n,d) \in S_{41}$, a contradiction.

The proof of (8.3.2) is similar to that of (8.3.1). Here we use the identity $2n+(n+3d)-3(n+d) = 0$ in place of (8.3.3). □

Now we turn to the proof of Theorem 1.5.1 for $k = 4$. We assume $P(\Delta) \leq 7$. In view of the case $k = 3$, we may assume that $7|n+d$ or $7|n+2d$. Thus $P(\Delta_1) \leq 5$ if $7|n+d$ and $P(\Delta_2) \leq 5$ if $7|n+2d$. Now we conclude from Lemma 8.3.1 that $(n,d) \in S_{41}$ if $7|n+d$ and $(n,d) \in S_{42}$ if $7|n+2d$. Finally we check that $P(\Delta) \geq 11$ for $(n,d) \in S_{41} \cup S_{42}$ unless $(n,d) \in \{(1,3),(1,13),(3,11)\}$. □

8.4. The cases $k = 6, 7, 9, 10$

We assume $P(\Delta) \leq 2k$. Further by Lemma 8.1.5, we may assume that

$$n + d > \begin{cases} 20 \cdot 3^5 & \text{if } k = 6, 7, \\ 40 \cdot 3^6 & \text{if } k = 9, 10. \end{cases} \tag{8.4.1}$$

There are at most $1 + [\frac{k-1}{p}]$ terms in Δ divisible by a prime p. After removing all the terms in Δ divisible by $p \geq 7$, we are left with at least 4 terms divisible by $2, 3$ and 5 only. After deleting the terms in which $2, 3, 5$ appear to maximal power, we are left with a term $n + i_0 d$ with $0 \leq i_0 < k$ such that $P(n + i_0 d) \leq 5$ and $n + i_0 d$ is at most $4 \cdot 3 \cdot 5$ if $k = 6, 7$; $8 \cdot 3 \cdot 5$ if $k = 9$ and $8 \cdot 9 \cdot 5$ if $k = 10$. If $i_0 > 0$, we get $n + d \leq 360$ contradicting (8.4.1). Thus we may suppose that $i_0 = 0$ and the terms in which $2, 3, 5$ appear to maximal power are different. Let $n + i_2 d$ and $n + i_3 d$ be the terms in which 2 and 3 appear to maximal power, respectively. Since 5 can divide at most 2 terms, we see that 5 can divide at most one of $n + i_2 d$ and $n + i_3 d$. Also $5 \nmid n$ if $5 | (n + i_2 d)(n + i_3 d)$. We write

$$n + i_2 d = 2^{\alpha_2} 3^{\beta_2} 5^{\gamma_2}, n + i_3 d = 2^{\alpha_3} 3^{\beta_3} 5^{\gamma_3} \tag{8.4.2}$$

with $(\gamma_2, \gamma_3) \in \{(0, 0), (1, 0), (0, 1)$. We observe that α_3 is at most 2 and 3 if $k = 6, 7$ and $k = 9, 10$, respectively, and β_2 is at most 1 and 2 if $k = 6, 7, 9$ and $k = 10$, respectively. If $k = 6, 7$, then $\alpha_2 \geq 7$ otherwise $n + d \leq n + i_2 d \leq 2^6 \cdot 3 \cdot 5$ contradicting (8.4.1). Similarly we derive $\beta_3 \geq 6$ if $k = 6, 7$ and $\alpha_2 \geq 8, \beta_3 \geq 7$ if $k = 9, 10$. From $i_3(n + i_2 d) - i_2(n + i_3 d) = (i_3 - i_2)n$, we get

$$i_3 2^{\alpha_2} 3^{\beta_2} 5^{\gamma_2} - i_2 2^{\alpha_3} 3^{\beta_3} 5^{\gamma_3} = (i_3 - i_2)n \tag{8.4.3}$$

Let

$$\alpha = \text{ord}_2 \left(\frac{i_3 2^{\alpha_2}}{i_2 2^{\alpha_3}} \right), \ \beta = \text{ord}_3 \left(\frac{i_2 3^{\beta_3}}{i_3 3^{\beta_2}} \right). \tag{8.4.4}$$

We show that $\alpha \geq \alpha_2 - \delta$ where $\delta = 2$ if $k = 6, 7$ and $\delta = 3$ if $k = 9, 10$. It suffices to prove $\text{ord}_2(\frac{i_3}{i_2 2^{\alpha_3}}) \geq -\delta$. If $\text{ord}_2(i_3) \geq \text{ord}_2(i_2)$, then it is clear. Thus we may assume that $\text{ord}_2(i_3) < \text{ord}_2(i_2)$. From (8.4.2), we get $(i_2 - i_3)d = 2^{\alpha_3}(2^{\alpha_2 - \alpha_3} O_2 - O_3)$ with O_2, O_3 odd. Therefore $\alpha_3 = \text{ord}_2(i_2 - i_3)$ since $\alpha_2 > \alpha_3$. Thus $\text{ord}_2(i_3) = \alpha_3$. Since $i_2 < k$, we get the desired inequality $\text{ord}_2(\frac{i_3}{i_2 2^{\alpha_3}}) \geq -\delta$. Hence $\alpha \geq \alpha_2 - \delta \geq 5$. Similarly we derive $\beta \geq 5$.

We obtain from (8.4.3) the equation

$$i 2^{\alpha} - j 3^{\beta} = t \tag{8.4.5}$$

with

$$\alpha \geq 5, \ \beta \geq 5, \tag{8.4.6}$$

$i, j \in \{1, 5, 7, 25, 35\}, t \in \{\pm 1, \pm 5, \pm 7, \pm 25, \pm 35\}$ and $\gcd(i, j) = \gcd(i, t) = \gcd(j, t) = 1$. From Lemmas 8.1.2, 8.1.3 and 8.1.4, we see that equations of the form

$$\begin{aligned} &2^{\alpha} - 3^{\beta} = \pm 1, && 2^{\alpha} - 3^{\beta} = \pm 5, \pm 25, \\ &2^{\alpha} - 5 \cdot 3^{\beta} = \pm 1, && 5 \cdot 2^{\alpha} - 3^{\beta} = \pm 1, \\ &2^{\alpha} - 25 \cdot 3^{\beta} = \pm 1, && 25 \cdot 2^{\alpha} - 3^{\beta} = \pm 1 \end{aligned}$$

are not possible by (8.4.6). Let the equations given by (8.4.5) be different from the above. Each of the equation gives rise to a Thue equality

$$X^3 + AY^3 = B \tag{8.4.7}$$

with integers $X, Y, A > 0, B > 0$ given by

	Equation	A	B	X	Y
(i)	$2^\alpha - 3^\beta = \pm 7$	$2^{a'}3^{b'}$	$7 \cdot 2^{a'}$	$\pm 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
(ii)	$7 \cdot 2^\alpha - 3^\beta = \pm 1, \pm 5, \pm 25$	$7 \cdot 2^{a'}3^{b'}$	$3^{b'}, 5 \cdot 3^{b'}, 25 \cdot 3^{b'}$	$\pm 3^{\frac{\beta+b'}{3}}$	$\pm 2^{\frac{\alpha-a'}{3}}$
(iii)	$2^\alpha - 7 \cdot 3^\beta = \pm 1, \pm 5, \pm 25$	$7 \cdot 2^{a'}3^{b'}$	$2^{a'}, 5 \cdot 2^{a'}, 25 \cdot 2^{a'}$	$\pm 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
(iv)	$25 \cdot 2^\alpha - 3^\beta = \pm 7$	$5 \cdot 2^{a'}3^{b'}$	$35 \cdot 2^{a'}$	$\pm 5 \cdot 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
(v)	$2^\alpha - 25 \cdot 3^\beta = \pm 7$	$5 \cdot 2^{a'}3^{b'}$	$35 \cdot 3^{b'}$	$\pm 5 \cdot 3^{\frac{\beta+b'}{3}}$	$\pm 2^{\frac{\alpha-a'}{3}}$
(vi)	$5 \cdot 2^\alpha - 7 \cdot 3^\beta = \pm 1$	$25 \cdot 7 \cdot 2^{a'}3^{b'}$	$25 \cdot 2^{a'}$	$\pm 5 \cdot 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
(vii)	$7 \cdot 2^\alpha - 5 \cdot 3^\beta = \pm 1$	$25 \cdot 7 \cdot 2^{a'}3^{b'}$	$25 \cdot 3^{b'}$	$\pm 5 \cdot 3^{\frac{\beta+b'}{3}}$	$\pm 2^{\frac{\alpha-a'}{3}}$
$(viii)$	$2^\alpha - 5 \cdot 3^\beta = \pm 7$	$5 \cdot 2^{a'}3^{b'}$	$7 \cdot 2^{a'}$	$\pm 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
(ix)	$5 \cdot 2^\alpha - 3^\beta = \pm 7$	$5 \cdot 2^{a'}3^{b'}$	$7 \cdot 3^{b'}$	$\pm 3^{\frac{\beta+b'}{3}}$	$\pm 2^{\frac{\alpha-a'}{3}}$
(x)	$35 \cdot 2^\alpha - 3^\beta = \pm 1$	$35 \cdot 2^{a'}3^{b'}$	$3^{b'}$	$\pm 3^{\frac{\beta+b'}{3}}$	$\pm 2^{\frac{\alpha-a'}{3}}$
(xi)	$2^\alpha - 35 \cdot 3^\beta = \pm 1$	$35 \cdot 2^{a'}3^{b'}$	$2^{a'}$	$\pm 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
(xii)	$2^\alpha - 3^\beta = \pm 35$	$2^{a'}3^{b'}$	$35 \cdot 2^{a'}$	$\pm 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$
$(xiii)$	$7 \cdot 2^\alpha - 25 \cdot 3^\beta = \pm 1$	$5 \cdot 7 \cdot 2^{a'}3^{b'}$	$5 \cdot 3^{b'}$	$\pm 5 \cdot 3^{\frac{\beta+b'}{3}}$	$\pm 2^{\frac{\alpha-a'}{3}}$
(xiv)	$25 \cdot 2^\alpha - 7 \cdot 3^\beta = \pm 1$	$5 \cdot 7 \cdot 2^{a'}3^{b'}$	$5 \cdot 2^{a'}$	$\pm 5 \cdot 2^{\frac{\alpha+a'}{3}}$	$\pm 3^{\frac{\beta-b'}{3}}$

where $0 \le a', b' < 3$ are such that X, Y are integers. Further

$$\max\{\mathrm{ord}_2(X), \mathrm{ord}_3(X)\} \ge 2, \ \max\{\mathrm{ord}_2(Y), \mathrm{ord}_3(Y)\} \ge 1 \tag{8.4.8}$$

by (8.4.6). Using Magma, we compute all the solutions in integers X, Y of the above Thue equations. We find that all the solutions of Thue equations other than (ii) and $(viii)$ do not satisfy (8.4.8). Further we check that the solutions of (ii) and $(viii)$ satisfy (8.4.8) but they do not satisfy (8.4.6). □

8.5. The cases $k = 12, 15, 16$

We assume $P(\Delta) \le 2k$. Let $k = 12, 15$. Then $P((n + d) \cdots (n + (k - 1)d)) \le 2k$. After deleting the terms from $\{n + d, \cdots, n + (k - 1)d\}$ divisible by primes p with $7 \le p \le 2k$, we get at least 4 terms $n + id$ composed of $2, 3$ and 5 only. This is also the case when $k = 16$ since 7 and 13 together divide at most 4 terms. Therefore there exists an i with $1 \le i \le k - 1$ such that $n + id$ divides $8 \cdot 9 \cdot 5$. Thus $n + d \le 360$. Now the assertion follows from Lemma 8.1.5. □

8.6. The case $k \ge 19$ with $2k - 1$ prime

It suffices to prove $W(\Delta) \ge \pi(2k) - \pi(k) + 1$ since $\pi(k) = \pi_d(k)$ by our assumption. We may suppose that $W(\Delta) = \pi(2k) - \pi(k)$ by Theorem 1.2.1. Further we observe that $d > 2k$ since $p(d) > 2k$.

By taking $m = \pi(2k) - \pi(k)$ in Lemma 7.1.2, we conclude that

$$d^{k-\pi(2k)-1} \le (k - 2) \cdots (k - \pi(2k)) \tag{8.6.1}$$

and hence

$$2k < d < (k - 2)^{\frac{\pi(2k)-1}{k-\pi(2k)-1}}. \tag{8.6.2}$$

Using Lemma 3.1.2, we see that

$$k - 2\pi(2k) \ge \frac{k}{\log 2k}\left(\log 2k - 4(1 + \frac{1.2762}{\log 2k})\right) \ge 0$$

for $k \ge 76$. With exact values of π function, we see that $k \ge 2\pi(2k)$ for $60 \le k < 76$. This implies $\pi(2k) - 1 \le k - \pi(2k) - 1$ for $k \ge 60$. Therefore for $k \ge 60$, we see that (8.6.2) does not hold. Thus $k < 60$. From (8.6.1), we see that $d \le 2k$ for $k \ge 30, k \ne 31$. Thus it remains to consider $k = 19, 21, 22, 24, 27, 31$. We see that $d \le 71$ if $k = 27, 31$; $d \le 83$ if $k = 19, 21$ and $d \le 113$ if $k = 22, 24$.

The next argument is analogous to (7.3.13) and (7.3.14) where $k-\pi(2k)+1$ has been replaced by $k-\pi(2k)$. Let n_e, d_e, n_o and d_o be positive integers with n_e even and n_o odd. For (n,d,k) with n even, $n \geq n_e, d \leq d_e$, we derive from (7.1.13) with $m=\pi(2k)-\pi(k)$ that

$$d^{k-\pi(2k)-1}\prod_{i=1}^{A_e-1}\left(\frac{n_e}{2d_e}+i\right)\prod_{j=1}^{k-\pi(2k)-A_e}\left(\frac{n_e}{d_e}+2j-1\right) \leq \min\left(1, \frac{k-1}{n_e}2^{-\theta+1}\right)(k-2)! \times 2^{\mathrm{ord}_2([\frac{k-2}{2}]!)-\mathrm{ord}_2((k-2)!)} \tag{8.6.3}$$

where A_e =min$(k-\pi(2k), \lceil\frac{2}{3}(k-\pi(2k))+\frac{n_e}{6d_e}-\frac{1}{3}\rceil)$, $\theta=1$ if k is odd, 0 otherwise. For (n,d,k) with n odd, $n \geq n_o, d \leq d_o$, we have

$$d^{k-\pi(2k)-1}\prod_{i=1}^{A_o}\left(\frac{n_o}{2d_o}+i-\frac{1}{2}\right)\prod_{j=1}^{k-\pi(2k)-A_o-1}\left(\frac{n_o}{d_o}+2j\right) \leq \min\left(1, \frac{k-1}{n_o}\right)(k-2)! \times 2^{\mathrm{ord}_2([\frac{k-2}{2}]!)-\mathrm{ord}_2((k-2)!)} \tag{8.6.4}$$

where A_o =min$(k-\pi(2k), \lceil\frac{2}{3}(k-\pi(2k))+\frac{n_o}{6d_o}-\frac{5}{6}\rceil)$. Here we have used $k-\pi(2k) \leq [\frac{k-2}{2}]$ for the expressions given by A_e and A_o. We take $n_e=2, n_o=1, d_e=d_o=83$ if $k=19,21,27,31$ and $n_e=2, n_o=1, d_e=d_o=113$ if $k=22,24$. We get a contradiction for $k=27,31$ since $d>2k$. Thus we may assume that $k \in \{19,21,22,24\}$. We obtain $d \leq D_e$ if n is even where $D_e=47,47,67$ and 61 according as $k=19,21,22$ and 24, respectively. If n is odd, then $d \leq D_o$ where $D_o=53,47,71$ and 67 according as $k=19,21,22$ and 24, respectively. By taking $n_e=4k, d_e=D_e$ and $n_o=4k+1, d_o=D_o$, we derive from (8.6.3) and (8.6.4) that $d<2k$. This is a contradiction. Thus $n<4k$. For these values of n,d and k, we check that $P(\Delta(n,d,k))>2k$ is valid. This completes the proof. □

Part 2

Proof of results on squares in products of terms in an arithmetic progression

CHAPTER 9

Notation, Preliminaries and General Lemmas

In this chapter, we define notation, preliminaries and general lemmas which will used in the following chapters.

9.1. Notations and Preliminaries

Let n, d, k, b, y be positive integers such that b is square free, $d \geq 1$, $k \geq 4$, $P(b) \leq k$ and $\gcd(n, d) = 1$. Let $t \leq k$ and $\gamma_1 < \gamma_2 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Let $\psi = k - t$. We consider the equation

$$(n + \gamma_1 d) \cdots (n + \gamma_t d) = by^2. \tag{9.1.1}$$

If $t = k$, we observe that $\gamma_i = i - 1$ and (9.1.1) coincides with (2.1.1). Assume that (9.1.1) holds. Then we have

$$n + \gamma_i d = a_{\gamma_i} x_{\gamma_i}^2 \text{ for } 1 \leq i \leq t \tag{9.1.2}$$

with a_{γ_i} squarefree such that $P(a_{\gamma_i}) \leq k$. Also

$$n + \gamma_i d = A_{\gamma_i} X_{\gamma_i}^2 \text{ for } 1 \leq i \leq t \tag{9.1.3}$$

$P(A_{\gamma_i}) \leq k$ and $\gcd(X_{\gamma_i}, \prod_{p \leq k} p) = 1$. Further we write

$$b_i = a_{\gamma_i},\ B_i = A_{\gamma_i},\ y_i = x_{\gamma_i},\ \ Y_i = X_{\gamma_i}.$$

Since $\gcd(n, d) = 1$, we see from (9.1.2) and (9.1.3) that

$$(b_i, d) = (B_i, d) = (y_i, d) = (Y_i, d) = 1 \text{ for } 1 \leq i \leq t. \tag{9.1.4}$$

By taking $m = n + \gamma_t d$ and $\gamma_i' = \gamma_t - \gamma_i$, we re-write (9.1.1) as

$$(m - \gamma_1' d) \cdots (m - \gamma_t' d) = by^2. \tag{9.1.5}$$

The equation (9.1.5) is called the mirror image of (9.1.1). The corresponding t-tuple $(a_{\gamma_1'}, a_{\gamma_2'}, \cdots, a_{\gamma_t'})$ is called the mirror image of $(a_{\gamma_1}, \cdots, a_{\gamma_t})$.

Let

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

For $b_i \in R$, let $\nu(b_i) = |\{j : 1 \leq j \leq t, b_j = b_i\}|$ and

$$\nu_o(b_i) = |\{j : 1 \leq j \leq t, b_j = b_i, 2 \nmid y_j\}|,\ \nu_e(b_i) = |\{j : 1 \leq j \leq t, b_j = b_i, 2|y_j\}|.$$

We define

$$R_\mu = \{b_i \in R : \nu(b_i) = \mu\},\ \ r_\mu = |R_\mu|,\ \ \mathfrak{r} = \big|\{(i, j) : b_i = b_j,\ b_i, b_j \in R \text{ and } i > j\}\big|.$$

Let

$$T = \{\gamma_i : Y_i = 1, 1 \leq i \leq t\},\ T_1 = \{\gamma_i : Y_i > 1, 1 \leq i \leq t\},\ S_1 = \{B_i : \gamma_i \in T_1\}.$$

Note that $Y_i > k$ for $i \in T_1$. For $i \in T_1$, we denote by $\nu(B_i) = |\{\gamma_j \in T_1 : B_j = B_i\}|$.

Let

$$\delta = \min(3, \mathrm{ord}_2(d)),\ \delta' = \min(1, \mathrm{ord}_2(d)), \tag{9.1.6}$$

$$\eta = \begin{cases} 1 & \text{if } \mathrm{ord}_2(d) \leq 1, \\ 2 & \text{if } \mathrm{ord}_2(d) \geq 2 \end{cases} \tag{9.1.7}$$

and

$$\rho = \begin{cases} 3 & \text{if } 3|d, \\ 1 & \text{if } 3 \nmid d. \end{cases} \tag{9.1.8}$$

Let $d^{'}\,|\,d$ and $d^{''} = \frac{d}{d^{'}}$ be such that $\gcd(d^{'}, d^{''}) = 1$. We write

$$d^{''} = d_1 d_2, \ \gcd(d_1, d_2) = \begin{cases} 1 & \text{if } \mathrm{ord}_2(d^{''}) \leq 1 \\ 2 & \text{if } \mathrm{ord}_2(d^{''}) \geq 2 \end{cases}$$

and we always suppose that d_1 is odd if $\mathrm{ord}_2(d^{''}) = 1$. We call such pairs (d_1, d_2) as partitions of $d^{''}$. We observe that the number of partitions of $d^{''}$ is $2^{\omega(d^{''})-\theta_1}$ where

$$\theta_1 := \theta_1(d^{''}) = \begin{cases} 1 & \text{if } \mathrm{ord}_2(d^{''}) = 1, 2 \\ 0 & \text{otherwise} \end{cases}$$

and we write θ for $\theta_1(d)$. In particular, by taking $d' = 1$ and $d^{''} = d$, the number of partitions of d is $2^{\omega(d)-\theta}$.

Let $b_i = b_j, i > j$. Then from (9.1.2) and (9.1.4), we have

$$\frac{(\gamma_i - \gamma_j)}{b_i} d^{'} = \frac{y_i^2 - y_j^2}{d^{''}} = \frac{(y_i - y_j)(y_i + y_j)}{d^{''}}. \tag{9.1.9}$$

such that $\gcd(d^{''}, y_i - y_j, y_i + y_j) = 1$ if $d^{''}$ is odd and 2 if $d^{''}$ is even. Thus a pair (i, j) with $i > j$ and $b_i = b_j$ corresponds to a partition (d_1, d_2) of $d^{''}$ such that $d_1 \mid (y_i - y_j)$, $d_2 \mid (y_i + y_j)$ and it is unique. Similarly, we have unique partition of $d^{''}$ corresponding to every pair (i, j) whenever $B_i = B_j$, $i, j \in T_1$.

Let $\mathfrak{p}_1 < \mathfrak{p}_2 < \cdots$ be the odd primes dividing d. Let

$$d = \begin{cases} 2^{\delta} \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_{\omega(d)-1} & \text{if } \delta = 1, 2 \\ \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_{\omega(d)} & \text{otherwise} \end{cases}$$

where $\mathfrak{q}_1 < \mathfrak{q}_2 < \cdots \mathfrak{q}_{\omega(d)-\theta}$ are prime powers dividing $\frac{d}{2^{\delta\theta}}$. By induction, we have

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_h \leq \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_h \leq \left(\frac{d}{2^{\delta\theta}} \right)^{\frac{h}{\omega(d)-\theta}} \tag{9.1.10}$$

for any h with $1 \leq h \leq \omega(d) - \theta$. Further we define

$$\mathcal{A}_h = \{B_i \in T_1 : B_i < \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_h\}, \quad \lambda_h = |\mathcal{A}_h|. \tag{9.1.11}$$

for any h with $1 \leq h \leq \omega(d) - \theta$.

We end this section with the following lemma.

Lemma 9.1.1. *Let ψ be fixed. Suppose that* (9.1.1) *with $P(b) \leq k$ has no solution at $k = k_1$ with k_1 prime. Then* (9.1.1) *with $P(b) \leq k$ has no solution at k with $k_1 \leq k < k_2$ where k_2 is the smallest prime larger than k_1.*

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

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

with $P(b) \leq k$. Then $P(b) \leq k_1$. We observe that $\gamma_{k_1-\psi} < k_1$ and by (9.1.2),

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

holds for some b' with $P(b') \leq k_1$ giving a solution of (9.1.1) at $k = k_1$. This is a contradiction. □

9.2. Some counting functions

Let p be a prime $\leq k$ and coprime to d. Then the number of i's for which b_i are divisible by q is at most

$$\sigma_q = \lceil \frac{k}{q} \rceil.$$

Let $r \geq 5$ be any positive integer. Define $F(k, r)$ and $F'(k, r)$ as

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

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

$$\mathcal{B}_r = \{b_i : P(b_i) \leq p_r\},\ I_r = \{i : b_i \in \mathcal{B}_r\} \text{ and } \xi_r = |I_r|.$$

We have

$$\xi_r \geq t - F(k, r) \geq t - F'(k, r) + \sum_{p|d, p>p_r} \sigma_p \tag{9.2.1}$$

and

$$t - |R| \geq t - |\{b_i : P(b_i) > p_r\}| - |\{b_i : P(b_i) \leq p_r\}| \tag{9.2.2}$$
$$\geq t - F(k, r) - |\{b_i : P(b_i) \leq p_r\}| \tag{9.2.3}$$
$$\geq t - F'(k, r) + \sum_{p|d, p>p_r} \sigma_p - |\{b_i : P(b_i) \leq p_r\}| \tag{9.2.4}$$
$$\geq t - F'(k, r) + \sum_{p|d, p>p_r} \sigma_p - 2^r. \tag{9.2.5}$$

We write $\mathcal{S} := \mathcal{S}(r)$ for the set of positive squarefree integers composed of primes $\leq p_r$. Let δ =min$\{3$,ord$_2(d)\}$. Let $p = q = 2^\delta$ or $p \leq q$ be odd primes dividing d. Let $p = q = 2^\delta$. Then $b_i \equiv n (\text{mod } 2^\delta)$. Considering modulo 2^δ for elements of $\mathcal{S}(r)$, we see by induction on r that

$$|\mathcal{B}_r| \leq 2^{r-\delta} =: g_{2^\delta, 2^\delta} =: g_{2^\delta}. \tag{9.2.6}$$

For any odd prime p dividing d, all b_i's are either quadratic residues mod p or non-quadratic residues mod p. For odd primes p, q dividing d with $p \leq q$, we consider four sets:

$$\begin{aligned}
\mathcal{S}_1(n', r) &= \mathcal{S}_1(\delta, n', p, q, r) = \{s \in \mathcal{S} : s \equiv n'(\text{mod } 2^\delta), \left(\frac{s}{p}\right) = 1, \left(\frac{s}{q}\right) = 1\},\\
\mathcal{S}_2(n', r) &= \mathcal{S}_2(\delta, n', p, q, r) = \{s \in \mathcal{S} : s \equiv n'(\text{mod } 2^\delta), \left(\frac{s}{p}\right) = 1, \left(\frac{s}{q}\right) = -1\},\\
\mathcal{S}_3(n', r) &= \mathcal{S}_3(\delta, n', p, q, r) = \{s \in \mathcal{S} : s \equiv n'(\text{mod } 2^\delta), \left(\frac{s}{p}\right) = -1, \left(\frac{s}{q}\right) = 1\},\\
\mathcal{S}_4(n', r) &= \mathcal{S}_4(\delta, n', p, q, r) = \{s \in \mathcal{S} : s \equiv n'(\text{mod } 2^\delta), \left(\frac{s}{p}\right) = -1, \left(\frac{s}{q}\right) = -1\}.
\end{aligned} \tag{9.2.7}$$

We take $n' = 1$ if $\delta = 0, 1$; $n' = 1, 3$ if $\delta = 2$ and $n' = 1, 3, 5, 7$ if $\delta = 3$. Then $\mathcal{B}_r \subseteq \mathcal{S}_j(n', r)$ for some n and some j with $1 \leq j \leq 4$. Let

$$g_{p,q} := g_{p,q}(r) = \max_{n'}(|\mathcal{S}_1(n', r)|, |\mathcal{S}_2(n', r)|, |\mathcal{S}_3(n', r)|, |\mathcal{S}_4(n', r)|) \tag{9.2.8}$$

and we write $g_p = g_{p,p}$. Then

$$|\mathcal{B}_r\}| \leq g_{p,q}. \tag{9.2.9}$$

In view of (9.2.6) and (9.2.9), the inequality (9.2.4) is improved as

$$t - |R| \geq t - F'(k,r) + \sum_{p|d, p>p_r} \sigma_p - \min_{p|d,q|d}\{g_{p,q}\}. \tag{9.2.10}$$

We observe that $\gcd(s,pq) = 1$ for $s \in \mathcal{S}_l$, $1 \leq l \leq 4$. Hence we see that $\mathcal{S}_l(n', r+1) = \mathcal{S}_l(n', r)$ if $p = p_{r+1}$ or $q = p_{r+1}$ implying

$$g_{p,q}(r+1) = g_{p,q}(r) \text{ if } p = p_{r+1} \text{ or } q = p_{r+1}. \tag{9.2.11}$$

Assume that $p_{r+1} \notin \{p,q\}$. Let $1 \leq l \leq 4$. We write $\mathcal{S}'_l(n', r+1) = \{s : s \in \mathcal{S}_l(n', r+1), p_{r+1}|s\}$. Then $s = p_{r+1}s'$ with $P(s') \leq p_r$ whenever $s \in \mathcal{S}'_l(n', r+1)$. Let $l = 1$. Then $s' \equiv n'p_{r+1}^{-1} \equiv n^{''}(\text{mod } 2^\delta)$ where $n^{''} = 1$ if $\delta = 0, 1$; $n^{''} = 1, 3$ if $\delta = 2$ and $n^{''} = 1, 3, 5, 7$ if $\delta = 3$. Further $\left(\frac{s'}{p}\right) = \left(\frac{p_{r+1}}{p}\right)$ and $\left(\frac{s'}{q}\right) = \left(\frac{p_{r+1}}{q}\right)$ for $s \in \mathcal{S}'_l(r+1)$. This implies $\mathcal{S}'_1(n', r+1) = p_{r+1}\mathcal{S}_m(n^{''}, r)$ for some $m, 1 \leq m \leq 4$. Therefore $|\mathcal{S}'_1(n', r+1)| \leq g_{p,q}(r)$ by (9.2.8). Similarly $|\mathcal{S}'_l(n', r+1)| \leq g_{p,q}(r)$ for each $l, 1 \leq 1 \leq 4$. Hence we get from $\mathcal{S}_l(n', r+1) = \mathcal{S}_l(n', r) \cup \mathcal{S}'_l(n', r+1)$ that

$$g_{p,q}(r+1) \leq 2g_{p,q}(r). \tag{9.2.12}$$

We now use the above assertions to calculate $g_{p,q}$.
i) Let $\delta = 0, r = 3, 4$ and $2 < p \leq 220$. Then

$$g_p(r) = \begin{cases} 2^{r-2} & \text{if } p \leq p_r \\ 2^{r-1} & \text{if } p > p_r \end{cases} \tag{9.2.13}$$

except when $r = 3, p \in \{71, 191\}$ where $g_p = 2^r$. *ii)* Let $5 \leq r \leq 7, p \leq 547$ when $\delta = 0, 1$; $5 \leq r \leq 7, p \leq 547$ when $\delta = 2$ and $5 \leq r \leq 7, p \leq 89$ when $\delta = 3$. Then

$$g_p(r) = \begin{cases} \max(1, 2^{r-\delta-2}) & \text{if } p \leq p_r \\ \max(1, 2^{r-\delta-1}) & \text{if } p > p_r \end{cases} \tag{9.2.14}$$

except when $\delta = 0, r = 5, p = 479$ where $g_p = 2^r$;
$\delta = 1, r = 5, p \in \{131, 421, 479\}$, $r = 6, p = 131$ where $g_p = 2^{r-\delta}$;
$\delta = 2, r = 5, p \in \{41, 101, 131, 331, 379, 421, 461, 479, 499\}$ where $g_p = 2^{r-\delta}$;
$\delta = 2, r = 6, p \in \{101, 131\}$, $r = 7, p = 101$ where $g_p = 2^{r-\delta}$;
$\delta = 3, r = 5, p = 3$ where $g_p = 2^{r-\delta-1}$, $r = 5, p = 41$ where $g_p = 2^{r-\delta}$.
iii) Let $5 \leq r \leq 7, p \leq 19, q \leq 193$, $23 \leq p < q \leq 97$ when $\delta = 0$ and $r = 5, 6, p < q \leq 37$ when $\delta \geq 1$. Then

$$g_{p,q}(r) = \begin{cases} \max(1, 2^{r-\delta-4}) & \text{if } p < q \leq p_r \\ \max(1, 2^{r-\delta-3}) & \text{if } p \leq p_r < q \\ \max(1, 2^{r-\delta-2}) & \text{if } p_r < p < q \end{cases} \tag{9.2.15}$$

except when

$$\delta=0 \text{ and } \begin{cases} r=5, & g_{p,q}=2^{r-2} \text{ for } (p,q)\in\{(5,43),(5,167),(7,113),(7,127),\\ & (7,137),(11,61),(11,179),(11,181)\};\\ r=5, & g_{p,q}=2^{r-1} \text{ for } (p,q)\in\{(19,139),(23,73),(37,83)\};\\ r=6, & g_{p,q}=2^{r-2} \text{ for } (p,q)=(7,137);\\ r=6, & g_{p,q}=2^{r-1} \text{ for } (p,q)=(37,83);\end{cases}$$

$$\delta=1 \text{ and } \begin{cases} r=5, & g_{p,q}=2^{r-4} \text{ for } (p,q)\in\{(5,7),(5,11)\};\\ r=5, & g_{p,q}=2^{r-3} \text{ for } (p,q)=(5,37);\\ r=5, & g_{p,q}=2^{r-2} \text{ for } (p,q)\in\{(13,23),(29,31)\};\\ r=6, & g_{p,q}=2^{r-4} \text{ for } (p,q)=(5,7);\end{cases}$$

$$\delta=2 \text{ and } \begin{cases} r=5, & g_{p,q}=2^{r-4} \text{ for } (p,q)\in\{(3,19),(5,17),(5,37),(7,13),\\ & (7,23),(7,29),(7,31),(11,19),(11,29),(11,31)\};\\ r=5, & g_{p,q}=2^{r-3} \text{ for } (p,q)\in\{(13,23),(17,37),(29,31)\};\\ r=6, & g_{p,q}=2^{r-5} \text{ for } (p,q)\in\{(5,7),(7,13)\};\\ r=6, & g_{p,q}=2^{r-4} \text{ for } (p,q)\in\{(7,29),(11,31),(13,23)\}.\end{cases}$$

Now we combine (9.2.14), (9.2.15), (9.2.12) and (9.2.11). We obtain (9.2.14) with $=$ replaced by $\leq$ for $r\geq 7$ and $p\leq 89$ and we shall refer it as (9.2.14, $\leq$). Further we obtain (9.2.15) with $=$ replaced by $\leq$ for $r\geq 7$ and either $p<q\leq 97$ when $\delta=0$ or $p=3, q=5$ when $\delta\geq 1$ and we shall refer it as (9.2.15, $\leq$).

9.3. Lemmas for the upper bound of $n+(k-1)d$

In this section, we assume that (9.1.1) holds. Let $i>j, g>h, 0\leq i,j,g,h<k$ be such that

$$b_i=b_j,\ b_g=b_h,\ \gamma_i+\gamma_j\geq\gamma_g+\gamma_h \tag{9.3.1}$$

and

$$y_i-y_j=d_1r_1,\ y_i+y_j=d_2r_2,\ y_g-y_h=d_1s_1,\ y_g+y_h=d_2s_2 \tag{9.3.2}$$

where (d_1,d_2) is a partition of d. We write $V(i,j,g,h,d_1,d_2)$ for such double pairs. We call $V(i,j,g,h,d_1,d_2)$ degenerate if

$$b_i=b_g, r_1=s_1 \text{ or } b_i=b_g, r_2=s_2. \tag{9.3.3}$$

Otherwise we call it non-degenerate. Let q_1 and q_2 be given by

$$|b_ir_1^2-b_gs_1^2|=q_1d_2 \text{ and } |b_ir_2^2-b_gs_2^2|=q_2d_1. \tag{9.3.4}$$

We shall also write $V(i,j,g,h,d_1,d_2)=V(i,j,g,h,d_1,d_2,q_1,q_2)$.

Let Ω be a set of pairs (i,j) with $i>j$ such that $b_i=b_j$. Then we say that Ω has *Property ND* if the the following holds: For any two distinct pairs (i,j) and (g,h) in Ω corresponding to a partition (d_1,d_2) of d, the double pair $V(i,j,g,h,d_1,d_2)$ is non-degenerate. We begin with the following lemma.

LEMMA 9.3.1. *Let* $d=\theta_1(k-1)^2, n=\theta_2(k-1)^3$ *with* $\theta_1>0$ *and* $\theta_2>0$. *Let* $V(i,j,g,h,d_1,d_2,q_1,q_2)$ *be a non-degenerate double pair. Then*

$$\theta_2<\frac{1}{2}\left\{\frac{1}{q_1q_2}-\theta_1+\sqrt{\frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}}\right\} \tag{9.3.5}$$

and

$$d_1<\frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)},\ d_2<\frac{4(k-1)}{q_2}. \tag{9.3.6}$$

Proof. We have from (9.3.2) that $y_i = \frac{d_1r_1+d_2r_2}{2}$ and $y_g = \frac{d_1s_1+d_2s_2}{2}$. Further from (9.1.2) and (9.3.1), we get

$$(\gamma_i - \gamma_g)d = b_iy_i^2 - b_gy_g^2 = \frac{1}{4}\left\{(b_ir_1^2 - b_gs_1^2)d_1^2 + (b_ir_2^2 - b_gs_2^2)d_2^2 + 2d(b_ir_1r_2 - b_gs_1s_2)\right\}.$$

We observe from (9.3.2), (9.3.1) and (9.1.2) that $b_ir_1r_2 = \gamma_i - \gamma_j, b_gs_1s_2 = \gamma_g - \gamma_h$. Therefore

$$2(\gamma_i + \gamma_j - \gamma_g - \gamma_h)d = (b_ir_1^2 - b_gs_1^2)d_1^2 + (b_ir_2^2 - b_gs_2^2)d_2^2. \tag{9.3.7}$$

Then reading modulo d_1, d_2 separately in (9.3.7), we have

$$\begin{aligned} d_2 \Big| (b_ir_1^2 - b_gs_1^2),\ d_1 \Big| (b_ir_2^2 - b_gs_2^2) \text{ if } \operatorname{ord}_2(d) \le 1 \\ \frac{d_2}{2} \Big| (b_ir_1^2 - b_gs_1^2),\ \frac{d_1}{2} \Big| (b_ir_2^2 - b_gs_2^2) \text{ if } \operatorname{ord}_2(d) \ge 2. \end{aligned} \tag{9.3.8}$$

Hence $2q_1, 2q_2$ are non-negative integers. We see that $q_1 \neq 0$ and $q_2 \neq 0$ since $V(i, j, g, h, d_1, d_2, q_1, q_2)$ is non-degenerate. Further we see from (9.1.2) that

$$b_iy_i^2 - b_gy_g^2 = (\gamma_i - \gamma_g)d, \quad b_jy_j^2 - b_hy_h^2 = (\gamma_j - \gamma_h)d. \tag{9.3.9}$$

Therefore, by (9.3.2), we have

$$\begin{aligned} 0 \neq F_1 := (b_ir_1^2 - b_gs_1^2)d_1^2 &= b_i(y_i - y_j)^2 - b_g(y_g - y_h)^2 \\ &= (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d - 2(b_iy_iy_j - b_gy_gy_h) \end{aligned} \tag{9.3.10}$$

and

$$\begin{aligned} 0 \neq F_2 := (b_ir_2^2 - b_gs_2^2)d_2^2 &= b_i(y_i + y_j)^2 - b_g(y_g + y_h)^2 \\ &= (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d + 2(b_iy_iy_j - b_gy_gy_h). \end{aligned} \tag{9.3.11}$$

We note here that $F_1 < 0, F_2 < 0$ is not possible since $\gamma_i + \gamma_j \ge \gamma_g + \gamma_h$.

Let a and b be positive real numbers with $a \neq b$. We have $2\sqrt{ab} = (a+b)(1 - (\frac{a-b}{a+b})^2)^{\frac{1}{2}}$. By using $1 - x < (1-x)^{\frac{1}{2}} < 1 - \frac{x}{2}$ for $0 < x < 1$, we get $a + b - \frac{(a-b)^2}{a+b} < 2\sqrt{ab} < a + b - \frac{(a-b)^2}{2(a+b)}$. We use it with $a = n + \gamma_id$ and $b = n + \gamma_jd$ so that $\sqrt{ab} = b_iy_iy_j$ by (9.1.2) and (9.3.1). We obtain

$$2n + (\gamma_i + \gamma_j)d - \frac{(\gamma_i - \gamma_j)^2d^2}{2n + (\gamma_i + \gamma_j)d} < 2b_iy_iy_j < 2n + (\gamma_i + \gamma_j)d - \frac{(\gamma_i - \gamma_j)^2d^2}{4n + 2(\gamma_i + \gamma_j)d}. \tag{9.3.12}$$

Similarly we get

$$2n + (\gamma_g + \gamma_h)d - \frac{(\gamma_g - \gamma_h)^2d^2}{2n + (\gamma_g + \gamma_h)d} < 2b_gy_gy_h < 2n + (\gamma_g + \gamma_h)d - \frac{(\gamma_g - \gamma_h)^2d^2}{4n + 2(\gamma_g + \gamma_h)d}. \tag{9.3.13}$$

Therefore we have from (9.3.4), (9.3.10), (9.3.12) and (9.3.13) that

$$\begin{aligned} q_1dd_1 <& (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d - (2n + (\gamma_i + \gamma_j)d) + \frac{(\gamma_i - \gamma_j)^2d^2}{2n + (\gamma_i + \gamma_j)d} \\ &+ (2n + (\gamma_g + \gamma_h)d) - \frac{(\gamma_g - \gamma_h)^2d^2}{4n + 2(\gamma_g + \gamma_h)d} \text{ if } F_1 > 0 \end{aligned}$$

and

$$\begin{aligned} q_1dd_1 <& (2n + (\gamma_i + \gamma_j)d) - \frac{(\gamma_i - \gamma_j)^2d^2}{4n + 2(\gamma_i + \gamma_j)d} - (2n + (\gamma_g + \gamma_h)d) \\ &+ \frac{(\gamma_g - \gamma_h)^2d^2}{2n + (\gamma_g + \gamma_h)d} - (\gamma_i + \gamma_j - \gamma_g - \gamma_h)d \text{ if } F_1 < 0. \end{aligned}$$

Thus

$$q_1d_1 < \begin{cases} \frac{(\gamma_i - \gamma_j)^2d}{2n + (\gamma_i + \gamma_j)d} = \frac{\theta_1(\gamma_i - \gamma_j)^2}{2\theta_2(k-1) + \theta_1(\gamma_i + \gamma_j)} & \text{if } F_1 > 0, \\ \frac{(\gamma_g - \gamma_h)^2d}{2n + (\gamma_g + \gamma_h)d} = \frac{\theta_1(\gamma_g - \gamma_h)^2}{2\theta_2(k-1) + \theta_1(\gamma_g + \gamma_h)} & \text{if } F_1 < 0. \end{cases} \tag{9.3.14}$$

Similarly from (9.3.4), (9.3.11), (9.3.12) and (9.3.13), we have

$$q_2d_2 < \begin{cases} 2(\gamma_i+\gamma_j-\gamma_g-\gamma_h)+\frac{\theta_1(\gamma_g-\gamma_h)^2}{2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h)} & \text{if } F_2>0 \\ \frac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)}-2(\gamma_i+\gamma_j-\gamma_g-\gamma_h) & \text{if } F_2<0. \end{cases} \tag{9.3.15}$$

Let

$$n_{i,j} := (k-1)^2\left\{\theta_2(k-1)+\frac{\theta_1(\gamma_i+\gamma_j)}{2}-\frac{\theta_1^2(\gamma_i-\gamma_j)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))}\right\}$$

and

$$n_{g,h} := (k-1)^2\left\{\theta_2(k-1)+\frac{\theta_1(\gamma_g+\gamma_h)}{2}-\frac{\theta_1^2(\gamma_g-\gamma_h)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h))}\right\}.$$

Then we see from (9.3.12) and (9.3.13) that $n_{i,j} < b_iy_iy_j < \frac{1}{4}b_i(y_i+y_j)^2$ and $n_{g,h} < b_gy_gy_h < \frac{1}{4}b_g(y_g+y_h)^2$, respectively. Assume $F_1>0$. Then from (9.3.4), (9.3.11) and (9.3.2), we have

$$n_{i,j}q_1d_2d_1^2 < \frac{1}{4}b_i(y_i+y_j)^2b_i(y_i-y_j)^2 = \frac{1}{4}(\gamma_i-\gamma_j)^2d^2$$

implying

$$\begin{aligned} \theta_1+\theta_2 &= \frac{n_{i,j}}{(k-1)^3}+\frac{\theta_1}{k-1}\left(k-1-\frac{\gamma_i+\gamma_j}{2}+\frac{\theta_1(\gamma_i-\gamma_j)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))}\right) \\ &< \frac{(\gamma_i-\gamma_j)^2}{4q_1(k-1)^3}d_2+\theta_1 \le \frac{d_2}{4q_1(k-1)}+\theta_1 \text{ if } F_1>0 \end{aligned} \tag{9.3.16}$$

by estimating $\frac{\theta_1(\gamma_i-\gamma_j)^2}{2(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))} \le \frac{(\gamma_i-\gamma_j)^2}{2(\gamma_i+\gamma_j)} < \frac{\gamma_i+\gamma_j}{2}$. Similarly

$$\theta_1+\theta_2 < \frac{d_2}{4q_1(k-1)}+\theta_1 \text{ if } F_1<0. \tag{9.3.17}$$

We separate the possible cases:
Case I: Let $F_1>0, F_2>0$. From (9.3.14) and (9.3.15), we have

$$\begin{aligned} q_1q_2\theta_1(k-1)^2 <& \frac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)}\left\{2(\gamma_i+\gamma_j-\gamma_g-\gamma_h)+\frac{\theta_1(\gamma_g-\gamma_h)^2}{2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h)}\right\} \\ <& \frac{\theta_1(\gamma_i-\gamma_j)^2}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)}\left\{2(\gamma_i+\gamma_j)-2(\gamma_g+\gamma_h)+\gamma_g-\gamma_h\right\} \\ <& \frac{2\theta_1(\gamma_i-\gamma_j)^2(\gamma_i+\gamma_j)}{2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j)} \le \frac{2\theta_1\gamma_i^3}{2\theta_2(k-1)+\theta_1\gamma_i} \le \frac{2\theta_1(k-1)^3}{2\theta_2(k-1)+\theta_1(k-1)} \end{aligned}$$

since $\frac{2\theta_1\gamma_i^3}{2\theta_2(k-1)+\theta_1\gamma_i^3}$ is an increasing function of γ_i. Therefore $2\theta_2+\theta_1 < \frac{2}{q_1q_2}$ which gives (9.3.5). Further from (9.3.14) and (9.3.15), we have

$$d_1 < \frac{\theta_1(\gamma_i-\gamma_j)^2}{q_1(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))} < \frac{\theta_1\gamma_i^2}{q_1(2\theta_2(k-1)+\theta_1\gamma_i)} \le \frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)}$$

and

$$d_2 < \frac{1}{q_2}\left\{2(\gamma_i+\gamma_j)-2(\gamma_g+\gamma_h)+\gamma_g-\gamma_h\right\} < \frac{2(\gamma_i+\gamma_j)}{q_2} < \frac{4(k-1)}{q_2}$$

giving (9.3.6).
Case II: Let $F_1>0, F_2<0$. From (9.3.14), we have

$$d_1 < \frac{\theta_1(\gamma_i-\gamma_j)^2}{q_1(2\theta_2(k-1)+\theta_1(\gamma_i+\gamma_j))} < \frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)}.$$

Similarly $d_2 < \frac{1}{q_2}\frac{\theta_1(k-1)}{2\theta_2+\theta_1} < \frac{k-1}{q_2}$ from (9.3.15) and $\gamma_i+\gamma_j \geq \gamma_g+\gamma_h$. Therefore (9.3.6) follows. Further

$$\theta_1(k-1)^2 = d = d_1d_2 < \frac{\theta_1^2(k-1)^2}{q_1q_2(2\theta_2+\theta_1)^2}$$

implying $(2\theta_2+\theta_1)^2 < \frac{\theta_1}{q_1q_2}$. Hence (9.3.5) follows.

Case III: Let $F_1<0, F_2>0$. From (9.3.14) and (9.3.15), we have

$$\theta_1(k-1)^2 < \frac{\theta_1\gamma_g^2}{q_1q_2(2\theta_2(k-1)+\theta_1\gamma_g)}\left\{2(\gamma_i+\gamma_j-\gamma_g)+\frac{\theta_1\gamma_g^2}{2\theta_2(k-1)+\theta_1\gamma_g}\right\}.$$

Let $\chi(\gamma_g) = 1-\frac{2\theta_2(k-1)}{2\theta_2(k-1)+\theta_1\gamma_g}$ so that $\gamma_g\chi(\gamma_g) = \frac{\theta_1\gamma_g^2}{2\theta_2(k-1)+\theta_1\gamma_g} \leq \frac{\theta_1(k-1)}{2\theta_2+\theta_1}$ and both $\chi(\gamma_g)$ and $\gamma_g\chi(\gamma_g)$ are increasing functions of γ_g. Since $\gamma_i+\gamma_j \leq 2(k-1)$, we have

$$\theta_1(k-1)^2 < \frac{\gamma_g\chi(\gamma_g)}{q_1q_2}\left\{2(2(k-1)-\gamma_g)+\gamma_g\chi(\gamma_g)\right\} = \frac{\chi(\gamma_g)}{q_1q_2}\left\{2\gamma_g(2(k-1)-\gamma_g)+\gamma_g^2\chi(\gamma_g)\right\}.$$

We see that $\gamma_g(2(k-1)-\gamma_g)$ is an increasing function of γ_g since $\gamma_g \leq k-1$. Therefore the right hand side of the above inequality is an increasing function of γ_g. Hence we obtain

$$\theta_1 < \frac{1}{(k-1)^2}\frac{\theta_1}{q_1q_2(2\theta_2+\theta_1)}\left\{2(k-1)^2+\frac{\theta_1(k-1)^2}{2\theta_2+\theta_1}\right\} = \frac{\theta_1}{q_1q_2(2\theta_2+\theta_1)}\left\{2+\frac{\theta_1}{2\theta_2+\theta_1}\right\}.$$

Thus $(2\theta_2+\theta_1)^2 < \frac{3\theta_1+4\theta_2}{q_1q_2}$. Then we derive

$$(2\theta_2+\theta_1-\frac{1}{q_1q_2})^2 < \frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}.$$

Thus we get either $2\theta_2+\theta_1 < \frac{1}{q_1q_2}$ or $2\theta_2+\theta_1-\frac{1}{q_1q_2} < \sqrt{\frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}}$ giving (9.3.5). Further from (9.3.14), we have

$$d_1 < \frac{\theta_1(\gamma_g-\gamma_h)^2}{q_1(2\theta_2(k-1)+\theta_1(\gamma_g+\gamma_h))} < \frac{\theta_1(k-1)}{q_1(2\theta_2+\theta_1)}.$$

As in Case I, we have $d_2 < \frac{4(k-1)}{q_2}$. Thus (9.3.6) follows. □

Let θ_1, θ_2 be as in as the statement of Lemma 9.3.1.

Corollary 9.3.2. *We have*

$$\theta_1 < \frac{3}{q_1q_2},\ \theta_1+\theta_2 < \theta_1+2\theta_2 < \frac{3}{q_1q_2}. \tag{9.3.18}$$

Proof. Since $\theta_2>0$, we see from (9.3.5) that either $\theta_1 < \frac{1}{q_1q_2}$ or $(\theta_1-\frac{1}{q_1q_2})^2 < \frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}$ giving $\theta_1 < \frac{3}{q_1q_2}$. Hence we get from (9.3.5) that

$$\theta_1+2\theta_2 < \frac{1}{q_1q_2}+\sqrt{\frac{1}{(q_1q_2)^2}+\frac{\theta_1}{q_1q_2}} < \frac{3}{q_1q_2}.$$

Thus (9.3.18) is valid. □

Lemma 9.3.3. *Let $b_i=b_j, b_g=b_h$ and $(d_1,d_2)\neq(\eta,\frac{d}{\eta})$ be a partition of d. Suppose that (i,j) and (g,h) correspond to the partitions (d_1,d_2) and (d_2,d_1), respectively. Then*

$$d_1 < \eta(k-1)^2,\ d_2 < \eta(k-1)^2. \tag{9.3.19}$$

Proof. We write

$$y_i-y_j = d_1r_1,\ y_i+y_j = d_2r_2,\ y_g-y_h = d_2s_2,\ y_g+y_h = d_1s_1.$$

with

$$b_ir_1r_2 = \gamma_i-\gamma_j, b_gs_1s_2 = \gamma_g-\gamma_h. \tag{9.3.20}$$

Then as in the proof of Lemma 9.3.1, we get (9.3.7) and (9.3.8). If both $b_ir_1^2 - b_gs_1^2 \neq 0$ and $b_ir_2^2 - b_gs_2^2 \neq 0$, we obtain $\max(d_1, d_2) < \eta \max(b_ir_1^2, b_gs_1^2, b_ir_2^2, b_gs_2^2) \leq \eta(k-1)^2$ by (9.3.20). Thus we may assume that either $b_ir_1^2 - b_gs_1^2 = 0$ or $b_ir_2^2 - b_gs_2^2 = 0$. Note that $b_ir_1^2 - b_gs_1^2 = b_ir_2^2 - b_gs_2^2 = 0$ is not possible. Suppose $b_ir_1^2 - b_gs_1^2 = b_ir_2^2 - b_gs_2^2 = 0$. Then $b_i = b_g, r_1 = s_1, r_2 = s_2$ implying $y_i = y_g, y_j = y_h$. Hence we get $\gamma_i = \gamma_g, \gamma_j = \gamma_h$ from (9.1.2) implying $(i, j) = (g, h)$ which is a contradiction. Now we consider the case $b_ir_1^2 - b_gs_1^2 = 0$ and the proof for the other is similar. From $b_ir_2^2 - b_gs_2^2 \neq 0$ and (9.3.7), we obtain $2(\gamma_i + \gamma_j - \gamma_g - \gamma_h)d_1 = (b_ir_2^2 - b_gs_2^2)d_2$ implying $d_1 \Big| \eta(b_ir_2^2 - b_gs_2^2)$ and $d_2 \Big| 2\eta(\gamma_i + \gamma_j - \gamma_g - \gamma_h)$. Hence by (9.3.20), $d_1 < \eta(k-1)^2, d_2 < 2\eta(k-1+k-2-1) \leq \eta(k-1)^2$ implying (9.3.19). □

For two pairs $(a, b), (c, d)$ with positive rationals a, b, c, d, we write $(a, b) \geq (c, d)$ if $a \geq c,\ b \geq d$.

Lemma 9.3.4. *Let (d_1, d_2) be a partition of d. Suppose that there is a set $\mathfrak{G}$ of at least z_0 distinct pairs corresponding to the partition (d_1, d_2) such that $V(i, j, g, h, d_1, d_2)$ is non-degenerate for any (i, j) and (g, h) in $\mathfrak{G}$. Then* (9.3.5), (9.3.6) *and* (9.3.18) *hold with $(q_1, q_2) \geq (Q_1, Q_2)$ where (Q_1, Q_2) is given by the following table.*

z_0	d *odd*	$2\|\|d$	$4\|\|d$	$8\|d$
2	$(1,1)$	$(2,1)$	$(\frac{1}{2},\frac{1}{2})$	$(1,\frac{1}{2})$ *if* $2\|\|d_1$, $(\frac{1}{2},1)$ *if* $2\|\|d_2$
3	$(2,2)$	$(4,4)$ *or* $(8,2)$	$(2,2)$	$(2,2)$
5	$(4,4)$	$(8,4)$	$(2,8)$ *or* $(8,2)$	$(2,8)$ *if* $2\|\|d_1$, $(8,2)$ *if* $2\|\|d_2$

Table 1

For example, $(Q_1, Q_2) = (1, 1)$ if $z_0 = 2, d$ odd and $(Q_1, Q_2) = (2, 2)$ if $z_0 = 3, 4||d$. If there exists a non-degenerate double pair $V(i, j, g, h, d_1, d_2)$, then we can apply Lemma 9.3.4 with $z_0 = 2$.

Proof. For any pair $(i, j) \in \mathfrak{G}$, we write

$$y_i - y_j = r_1(i,j)d_1 \quad \text{and} \quad y_i + y_j = r_2(i,j)d_2 \tag{9.3.21}$$

where $r_1 = r_1(i, j)$ and $r_2 = r_2(i, j)$ are integers.

Let d be odd. Then $r_1 \equiv r_2 (\text{mod } 2)$ for any pair (i, j) by (9.3.21) and we shall use it in this paragraph without reference. We observe that $q_1 \geq 1, q_2 \geq 1$ by (9.3.8), (9.3.4) and the assertion follows for $z_0 = 2$. Let $z_0 = 3$. If there are two distinct pairs (i, j) with b_ir_1 even, then $q_1 \geq 2, q_2 \geq 2$ by (9.3.8). Thus we may assume that there is at most one pair (i, j) for which b_ir_1 is even. Therefore, for the remaining two pairs, we see that both b_ir_1's are odd and the assertion follows again by (9.3.8). Let $z_0 = 5$. We may suppose that there is at most one (i, j) for which r_1 is even otherwise the result follows from (9.3.8). Now we consider remaining four pairs (i, j) for which $r_1^2 \equiv 1(\text{mod } 4)$. Out of these pairs, there are (i_1, j_1) and (i_2, j_2) such that $b_{i_1} \equiv b_{i_2} (\text{mod } 4)$ since b's are square free. Now the assertion follows from (9.3.8).

Let d be even. We observe that

$$8|(y_i^2 - y_j^2) \text{ and } \gcd(y_i - y_j, y_i + y_j) = 2 \tag{9.3.22}$$

for any pair (i, j). Let $2||d$. Then d_1 is odd and d_2 is even implying r_1 is even by (9.3.22). Further from (9.3.22), we have either $4|r_1, 2 \nmid r_2$ or $2||r_1, 2|r_2$. Therefore $(q_1, q_2) \geq (2, 1)$ by (9.3.8) since r_1 is even and the assertion follows for $z_0 = 2$. Let $z_0 = 3$. Then there are two pairs (i_1, j_1) and (i_2, j_2) such that $r_2(i_1, j_1) \equiv r_2(i_2, j_2)(\text{mod } 2)$. Assume that r_2 is odd. Then $4|r_1$ which implies $8|q_1$ and $2|q_2$ by (9.3.8). Now we suppose that r_2 is even. Then $2||r_1$. We write $r_1 = 2r_1'$ and

$$b_{i_1}r_1^2(i_1, j_1) - b_{i_2}r_1^2(i_2, j_2) = 4(b_{i_1}r_1'^2(i_1, j_1) - b_{i_2}r_1'^2(i_2, j_2)) \equiv 0(\text{mod } 8).$$

Hence $4|q_1$, $4|q_2$ by (9.3.8). Let $z_0 = 5$. We choose three pairs (i, j) for which all b_i's $\equiv 1(\text{mod } 4)$ or all b_i's $\equiv 3(\text{mod } 4)$. Out of these, we choose two pairs both of which satisfy either $4|r_1, 2 \nmid r_2$ or $2||r_1, 2|r_2$. Now we argue as above and use $b_{i_1} \equiv b_{i_2} (\text{mod } 4)$ to get the result.

Let $4||d$. Then both d_1 and d_2 are even. From (9.3.22), we have either $2|r_1, 2 \nmid r_2$ or $2 \nmid r_1, 2|r_2$. Since $(q_1, q_2) \geq (\frac{1}{2}, \frac{1}{2})$ by (9.3.8), the the assertion follows for $z_0 = 2$. Let $z_0 = 3$. Then there are two pairs (i_1, j_1) and (i_2, j_2) such that $r_1(i_1, j_1) \equiv r_1(i_2, j_2)(\text{mod } 2)$ and $r_2(i_1, j_1) \equiv r_2(i_2, j_2)$(mod

2). Since $b_i \equiv n(\text{mod } 4)$ for each i, we get from (9.3.8) and (9.3.4) that $2|q_1$ and $2|q_2$. Thus $(q_1, q_2) \geq (2, 2)$. Let $z_0 = 5$. Then we get 3 pairs (i, j) for which $2|r_1(i, j), 2 \nmid r_2(i, j)$ or 3 pairs (i, j) for which $2 \nmid r_1(i, j), 2|r_2(i, j)$. Assume the first case. Then there are 2 pairs (i_1, j_1) and (i_2, j_2) such that $r_1(i_1, j_1) \equiv r_1(i_2, j_2)(\text{mod } 4)$. This, with $b_i \equiv n(\text{mod } 4)$ and (9.3.4), implies that $16|q_1d_2$ and $4|q_2d_1$. Hence $(q_1, q_2) \geq (8, 2)$. In the latter case, we get $(q_1, q_2) \geq (2, 8)$ similarly.

Let $8|d$. Then we have from (9.3.21) and (9.3.22) that either $2||d_1$ implying all r_1's are odd, or $2||d_2$ implying all r_2's are odd. Also $b_i \equiv n(\text{mod } 8)$ for all i. We prove the result for $2||d_1$ and the proof for the other case is similar. From (9.3.7), we derive

$$(9.3.23) \qquad 2(\gamma_{i_1} + \gamma_{j_1} - \gamma_{i_2} - \gamma_{j_2})\frac{d_1}{2}\frac{d_2}{2} = (b_{i_1}r_1^2 - b_{i_2}s_1^2)\left(\frac{d_1}{2}\right)^2 + (b_{i_1}r_2^2 - b_{i_2}s_2^2)\left(\frac{d_2}{2}\right)^2$$

where $r_1 = r_1(i_1, j_1), s_1 = r_1(i_2, j_2), r_2 = r_2(i_1, j_1)$ and $s_2 = r_2(i_2, j_2)$. Noting that $4d_2|d_2^2$ and taking modulo d_2, we get $(q_1, q_2) \geq (1, \frac{1}{2})$ implying the assertion for $z_0 = 2$. Let $z_0 = 3$. Then there are 2 pairs (i_1, j_1) and (i_2, j_2) such that $r_2(i_1, j_1) \equiv r_2(i_2, j_2)(\text{mod } 2)$. Using this and (9.3.4), we get $4|q_2d_1$. Further from $b_ir_1r_2 = \gamma_i - \gamma_j$, we see that $\gamma_{i_1} - \gamma_{j_1} \equiv \gamma_{i_2} - \gamma_{j_2}(\text{mod } 2)$ implying $\gamma_{i_1} + \gamma_{j_1} \equiv \gamma_{i_2} + \gamma_{j_2}(\text{mod } 2)$. Now we see from (9.3.23) that $4\frac{d_2}{2}|q_1d_2$. Thus $(q_1, q_2) \geq (2, 2)$. Let $z_0 = 5$. We see that $b_i \equiv n$ or $n{+}8$ modulo 16 so that $b_ir_2^2(\text{mod } 16)$ is equal to 0 if $4|r_2$, $4n$ if $2||r_2$ and $n, n{+}8$ if $2 \nmid r_2$. Now we can find 2 pairs (i_1, j_1) and (i_2, j_2) such that $b_{i_1}r_2^2(i_1, j_1) \equiv b_{i_2}r_2^2(i_2, j_2)$(mod 16). This gives $16|q_2d_1$ by (9.3.4). Further again $2|(\gamma_{i_1} + \gamma_{j_1} - \gamma_{i_2} - \gamma_{j_2})$ and hence $4\frac{d_2}{2}|q_1d_2$ from (9.3.23). Therefore $(q_1, q_2) \geq (2, 8)$. □

Lemma 9.3.5. *(i) Assume that*

$$(9.3.24) \qquad n + \gamma_t d > \eta^2\gamma_t^2.$$

Then for any pair (i, j) with $b_i = b_j$, the partition $(d\eta^{-1}, \eta)$ is not possible.
(ii) Let $d = d^{'}d^{''}$ with $\gcd(d^{'}, d^{''}) = 1$. Then for any pair (i, j) with $B_i = B_j \geq d^{'}$, $i, j \in T_1$, the partition $(d^{''}\eta^{-1}, \eta)$ is not possible. In particular, the partition $(d\eta^{-1}, \eta)$ is not possible.

Proof. (i) Suppose the pair (i, j) with $b_i = b_j$ correspond to the partition $(d\eta^{-1}, \eta)$. From $\frac{n+\gamma_i d}{n+\gamma_t d} > \frac{\gamma_i}{\gamma_t}$ and (9.3.24), we get $n + \gamma_i d > \eta^2\gamma_i\gamma_t$. Then from (9.1.9), we have

$$\gamma_i - \gamma_j \geq \frac{b_i(y_i + y_j)}{\eta} \geq \frac{(b_iy_i^2)^{\frac{1}{2}} + (b_jy_j^2)^{\frac{1}{2}}}{\eta} > \frac{\eta(\sqrt{\gamma_i\gamma_t} + \sqrt{\gamma_j\gamma_t})}{\eta} \geq \gamma_i + \gamma_j,$$

a contradiction.
(ii) Suppose the pair (i, j) with $B_i = B_j \geq d^{'}$ correspond to the partition $(d^{''}\eta^{-1}, \eta)$. As in (9.1.9), we have

$$\gamma_i - \gamma_j \geq (\gamma_i - \gamma_j)\frac{d^{'}}{B_i} \geq \frac{Y_i + Y_j}{\eta} > \frac{2k}{2}$$

since $Y_i \geq Y_j > k$. This is a contradiction. The latter assertion follows by taking $d^{'} = 1, d^{''} = d$. □

Lemma 9.3.6. *(i) Assume (9.3.24). Let $1 \leq i_0 \leq t$ and $\nu(b_{i_0}) = \mu$. Let (d_1, d_2) be any partition of d. Then the number of pairs (i, j) with $b_i{=}b_j{=}b_{i_0}, i > j$ corresponding to (d_1, d_2) is at most $[\frac{\mu}{2}]$.*
(ii) Let $d = d^{'}d^{''}$ with $\gcd(d^{'}, d^{''}) = 1$. Let $i_0 \in T_1$, $B_{i_0} \geq d^{'}$ and $\nu(B_{i_0}) = \mu$. Let (d_1, d_2) be any partition of $d^{''}$. Then the number of pairs (i, j) with $B_i{=}B_j{=}B_{i_0}, i > j$ corresponding to (d_1, d_2) is at most $[\frac{\mu}{2}]$.

Proof. (i) Suppose there are $\mu' = [\frac{\mu}{2}]{+}1$ pairs (i_l, j_l) with $i_l > j_l, 0 \leq l < \mu'$ and $b_{i_l} = b_{j_l} = b_{i_0}$ corresponding to (d_1, d_2). We consider the sets $I = \{i_l | 0 \leq l < \mu'\}$ and $J = \{j_l | 0 \leq l < \mu'\}$. If $|I| < \mu'$ or $|J| < \mu'$ or $I \cap J \neq \phi$, then there are $l \neq m$ such that

$$d_1|(y_{j_l} - y_{j_m}),\ d_2|(y_{j_l} - y_{j_m}) \text{ if } i_l = i_m$$
$$d_1|(y_{i_l} - y_{i_m}),\ d_2|(y_{i_l} - y_{i_m}) \text{ if } j_l = j_m$$
$$d_1|(y_{j_l} - y_{i_m}),\ d_2|(y_{j_l} - y_{i_m}) \text{ if } i_l = j_m.$$

We exclude the first possibility and proofs for the others are similar. Without loss of generality, we may assume that $j_l > j_m$. Then $\mathrm{lcm}(d_1, d_2)\big|(y_{j_l} - y_{j_m})$ so that the pair (j_l, j_m) correspond to the partition $(d\eta^{-1}, \eta)$. This is not possible by Lemma 9.3.5 (i). Thus $|I| = \mu'$, $|J| = \mu'$ and $I \cap J = \phi$. Now we see that $|I \cup J| = |I| + |J| = 2\mu' > \mu$ and $b_i = b_{i_0}$ for every $i \in I \cup J$. This contradicts $\nu(b_{i_0}) = \mu$.
(ii) The proof is similar to that of (i) and we use Lemma 9.3.5 (ii). □

As a corollary, we have

Corollary 9.3.7. *(i) Assume* (9.3.24)*. For* $1 \leq i \leq t$*, we have* $\nu(b_i) \leq 2^{\omega(d)-\theta}$*.*
(ii) Let $d = d^{'}d^{''}$ *with* $\gcd(d^{'}, d^{''}) = 1$*. For* $B_i \geq d^{'}$*, we have* $\nu(B_i) \leq 2^{\omega(d^{''})-\theta_1}$*. In particular,* $\nu(B_i) \leq 2^{\omega(d)-\theta}$*.*

Proof. (i) Let $\nu(b_i) = \mu$. Then there are $\frac{\mu(\mu-1)}{2}$ pairs (g, h) with $g > h$ and $b_g = b_h = b_i$. Since there are at most $2^{\omega(d)-\theta} - 1$ permissible partitions of d, we see from Lemma 9.3.6 (i) that $\frac{\mu(\mu-1)}{2} \leq \frac{\mu}{2}(2^{\omega(d)-\theta} - 1)$. Hence the assertion follows.
(ii) The proof of the assertion (ii) is similar and we use Lemma 9.3.6 (ii). □

Corollary 9.3.8. *Let* $T_{h+1} = \{i \in T_1 : B_i \geq \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_h\}$ *and* $s_{h+1} = |\{B_i : i \in T_{h+1}\}|$*. Then*

$$|T_{h+1}| \geq |T_1| - \sum_{\mu=1}^{h-1} 2^{\omega(d)-\mu-\theta}\lambda_\mu - 2^{\omega(d)-h-1-\theta}\lambda_h$$

and

$$s_{h+1} \geq \frac{|T_1|}{2^{\omega(d)-h-\theta}} - \sum_{\mu=1}^{h-1} 2^{h-\mu}\lambda_\mu - 2\lambda_h$$

where λ*'s are as defined in* (9.1.11)*.*

Proof. We apply Corollary 9.3.7 *(ii)* with $d' = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_\mu$ to derive that $\nu(B_i) \leq 2^{\omega(d)-\mu-\theta}$ for $B_i \geq \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_\mu$, $\mu \geq 1$ since $\theta_1 \geq \theta$. Therefore

$$|T_{h+1}| \geq |T_1| - 2^{\omega(d)-\theta}\lambda_1 - 2^{\omega(d)-1-\theta}(\lambda_2 - \lambda_1) - \cdots - 2^{\omega(d)-h+1-\theta}(\lambda_h - \lambda_{h-1}).$$

and the first assertion follows. Further from $\nu(B_i) \leq 2^{\omega(d)-h-\theta}$ for $i \in T_{h+1}$, we have $s_{h+1} \geq \frac{|T_{h+1}|}{2^{\omega(d)-h-\theta}}$ and the last assertion follows. □

Lemma 9.3.9. *Assume* (9.3.24)*. There exists a set* Ω *of at least*

$$t - |R| + \sum_{\substack{\mu>1 \\ \mu \text{ odd}}} r_\mu \geq t - |R|$$

pairs (i, j) *having Property ND.*

Proof. We have

$$t = \sum_\mu \mu r_\mu \text{ and } |R| = \sum_\mu r_\mu.$$

Each $b_{i_0} \in R_\mu$ gives rise to $\frac{\mu(\mu-1)}{2}$ pairs (i, j) with $i > j$ such that $b_i = b_j = b_{i_0}$ and each pair corresponds to a partition of d. By Lemma 9.3.6, we know that there are at most $[\frac{\mu}{2}]$ pairs corresponding to any partition of d. For each $1 \leq j \leq [\frac{\mu}{2}] = \mu_1$, let v_j be the number of partitions of d for which there are j pairs out of the ones given by $b_{i_0} \in R_\mu$ corresponding to that partition. Then

$$\frac{\mu(\mu-1)}{2} = \sum_{j=1}^{\mu_1} jv_j. \tag{9.3.25}$$

For each partition having j pairs with $v_j > 0$, we remove $j-1$ pairs. Then we remove in all $\sum_{j=1}^{\mu_1}(j-1)v_j$ pairs. Rewriting (9.3.25) as

$$\frac{\mu(\mu-1)}{2} = \mu_1 \sum_{j=1}^{\mu_1} v_j - \sum_{j=1}^{\mu_1}(\mu_1 - j)v_j,$$

we see that we are left with at least

$$\sum_{j=1}^{\mu_1} v_j = \frac{\mu(\mu-1)}{2\mu_1} + \sum_{j=1}^{\mu_1}(1-\frac{j}{\mu_1})v_j \geq \frac{\mu(\mu-1)}{2\mu_1} = \begin{cases} \mu - 1 & \text{if } \mu \text{ is even} \\ \mu & \text{if } \mu \text{ is odd} \end{cases}$$

pairs. Let Ω be the union of all such pairs taken over all $b_{i_0} \in R_\mu$ and for all $\mu \geq 2$. Since $|R_\mu| = r_\mu$, we have

$$|\Omega| \geq \sum_{\mu \text{ even}} (\mu-1)r_\mu + \sum_{\substack{\mu>1 \\ \mu \text{ odd}}} \mu r_\mu = t - |R| + \sum_{\substack{\mu>1 \\ \mu \text{ odd}}} r_\mu.$$

Further we see from the construction of the set Ω that Ω satisfy *Property ND.* □

COROLLARY 9.3.10. *Assume* (9.3.24). *Let z be a positive integer and $\mathfrak{h}(z) = (z-1)(2^{\omega(d)-\theta} - 1) + 1$. Let $z_0 \in \{2,3,5\}$. Suppose that $t - |R| \geq \mathfrak{h}(z_0)$. Then there exists a partition (d_1, d_2) of d such that* (9.3.5), (9.3.6) *and* (9.3.18) *hold with $(q_1, q_2) \geq (Q_1, Q_2)$ where (Q_1, Q_2) is given by Table 1.*

PROOF. By Lemma 9.3.9, there exists a set Ω with at least $\mathfrak{h}(z_0)$ pairs satisfying *Property ND.* Since there are at most $2^{\omega(d)-\theta} - 1$ permissible partitions of d by Lemma 9.3.5 (i), we can find a partition (d_1, d_2) of d and a subset $\mathfrak{G} \subset \Omega$ of at least z_0 pairs corresponding to (d_1, d_2). Now the result follows by Lemma 9.3.4. □

COROLLARY 9.3.11. *Assume* (9.3.24). *Suppose that $t - |R| \geq 2^{\omega(d)-\theta-1} + 1$. Then there exists a partition (d_1, d_2) of d such that* (9.3.19) *holds.*

PROOF. By Lemma 9.3.9, there exists a set Ω with at least $2^{\omega(d)-\theta-1} + 1$ pairs (i,j) satisfying *Property ND.* We may assume that for each partition (d_1, d_2) of d, there is at most 1 pair corresponding to (d_1, d_2) otherwise the assertion follows by $z_0 = 2$ in Lemma 9.3.4. We see that there are $2^{\omega(d)-\theta-1} - 1$ partitions (d_1, d_2) with $d_1 > d_2$, $2^{\omega(d)-\theta-1} - 1$ partitions (d_1, d_2) with $\eta < d_1 < d_2$ and the partition $(\eta, d\eta^{-1})$. Since there are at least $2^{\omega(d)-\theta-1} + 1$ pairs, we can find two pairs (i,j) and (g,h) corresponding to the partitions (d_1, d_2) and (d_2, d_1), respectively. Now the assertion follows by Lemma 9.3.3. □

LEMMA 9.3.12. *Assume* (9.3.24).
(i) *Let $|S_1| \leq |T_1| - \mathfrak{h}(3)$. Then* (9.3.18) *is valid with*

$$q_1 q_2 \geq \begin{cases} 144\rho^{-1} & \text{if } 2 \nmid d \\ 16 & \text{if } 2 || d \\ 4 & \text{if } 4 | d. \end{cases} \tag{9.3.26}$$

(ii) *Let d be even and $|S_1| \leq |T_1| - \mathfrak{h}(5)$. Then* (9.3.18) *is valid with*

$$q_1 q_2 \geq \begin{cases} 144\rho^{-1} & \text{if } 2 || d \\ 36 & \text{if } 4 | d \text{ and } 3 \nmid d \\ 16 & \text{if } 4 | d \text{ and } 3 | d. \end{cases} \tag{9.3.27}$$

PROOF. Let $B_i = B_j$ with $i > j$ and $i, j \in T_1$. Then there is a partition (d_1, d_2) of d such that $Y_i - Y_j = d_1 r_1'$, $Y_i + Y_j = d_2 r_2'$ with r_1', r_2' even, $24\rho^{-1} | r_1' r_2'$ if d is odd and r_1' even, $12\rho^{-1} | r_1' r_2'$ if $2 || d$ and $3\rho^{-1} | r_1' r_2'$ if $4 | d$. Since $B_i Y_i^2 = b_i y_i^2$ and b_i is squarefree, we see that $p | b_i$ if and only if $p | B_i$ with $\text{ord}_p(B_i)$ odd. Therefore $b_i = b_j$ implying $b^2 = \frac{B_i}{b_i} = \frac{B_j}{b_j}$ and $y_i = bY_i, y_j = bY_j$. Hence

$$y_i - y_j = d_1 b r_1' = d_1 r_1(i,j) = d_1 r_1, \ \ y_i + y_j = d_2 b r_2' = d_2 r_2(i,j) = d_2 r_2$$

with $r_1 = br_1', r_2 = br_2'$ even, $24\rho^{-1}|r_1r_2$ if d is odd; r_1 even, $12\rho^{-1}|r_1r_2$ if $2||d$ and $3\rho^{-1}|r_1r_2$ if $4|d$. Let $z \in \{3,5\}$ and $|S_1| \le |T_1| - \mathfrak{h}(z)$. We argue as in Lemma 9.3.9 and Corollary 9.3.10 with t and $|R|$ replaced by $|T_1|$ and $|S_1|$. There exists a partition (d_1,d_2) of d and z pairs corresponding to (d_1,d_2) such that $V(i,j,g,h,d_1,d_2)$ is non-degenerate for any two such distinct pairs (i,j) and (g,h). Let $z=3$. By Lemma 9.3.4 with $z_0=3$, we may suppose that d is odd. Let $3 \nmid d$. Then we can find two distinct pairs (i_1,j_1) and (i_2,j_2) both of which satisfy either $3|r_1(i_1,j_1)$, $3|r_1(i_2,j_2)$ or $3|r_2(i_1,j_1), 3|r_2(i_2,j_2)$. Now (9.3.26) follows from (9.3.8) and (9.3.4) since r_1,r_2 are even. Assume that $3|d$. Let $3|d_1$. Then we can find two distinct pairs (i_1,j_1) and (i_2,j_2) both of which satisfy either $3|r_1(i_1,j_1)$, $3|r_1(i_2,j_2)$ or $3 \nmid r_1(i_1,j_1)$, $3 \nmid r_1(i_2,j_2)$. Since $b_i \equiv n(\text{mod } 3)$ and $r^2 \equiv 1(\text{mod } 3)$ for $3 \nmid r$, the assertion follows from (9.3.8) and (9.3.4) since r_1,r_2 are even. The same assertion hold for $3|d_2$ in which case r_1 is replaced by r_2. This proves (9.3.26) and we turn to the proof of (9.3.27). Let d be even and $z=5$. Let $3 \nmid d$. Out of these five pairs, we can find three distinct pairs (i,j) for which either $r_1(i,j)$'s are all divisible by 3 or $r_2(i,j)$'s are all divisible by 3. As in the proof of Lemma 9.3.4 with d even and $z_0=3$, we find two distinct pairs (i_1,j_1) and (i_2,j_2) such that $16|q_1q_2$ if $2||d$ and $4|q_1q_2$ if $4|d$. Further $9|q_1q_2$ since either $r_1(i,j)$'s are all divisible by 3 or $r_2(i,j)$'s are all divisible by 3 and hence the assertion. Assume now that $3|d$. By Lemma 9.3.4 with $z_0=5$, we may suppose that $2||d$. Let $3|d_1$. Then we can find three pairs (i,j) for which either 3 divides all $r_1(i,j)$'s or 3 does not divide any $r_1(i,j)$. Then for any two such pairs (i_1,j_1) and (i_2,j_2), we have $3|(b_{i_1}r_1^2(i_1,j_1) - b_{i_2}r_1^2(i_2,j_2))$. Therefore by the proof of Lemma 9.3.4 with d even and $z_0=3$, we get $3\cdot 16|q_1q_2$. The other case $3|d_2$ is similar. □

The next result depends on an idea of Erdős and Rigge.

Lemma 9.3.13. *Let* $z_1 > 1$ *be a real number,* $h_0 > i_0 \ge 0$ *be integers such that* $\prod_{b_i \in R} b_i \ge z_1^{|R|-i_0}(|R|-i_0)!$ *for* $|R| \ge h_0$*. Suppose that* $t - |R| < g$ *and let* $g_1 = k - t + g - 1 + i_0$*. For* $k \ge h_0 + g_1$ *and for any real number* $\mathfrak{m} > 1$*, we have*

$$g_1 > \frac{k\log\left(\frac{z_1\mathfrak{n}_0}{2.71851}\prod\limits_{p\le\mathfrak{m}} p^{\frac{2}{p^2-1}(1-\frac{1}{p^{\mathfrak{n}(k,p)}})}\right) + (k+\frac{1}{2})\log(1-\frac{g_1}{k})}{\log(k-g_1)-1+\log z_1} + \tag{9.3.28}$$
$$\frac{(.5\ell+1)\log k - \log\left(\mathfrak{n}_1^{-1}\prod\limits_{p\le\mathfrak{m}} p^{1.5\mathfrak{n}(k,p)}\right)}{\log(k-g_1)-1+\log z_1}$$

and

$$g_1 > \frac{k\log\left(\frac{z_1\mathfrak{n}_0}{2.71851}\prod\limits_{p\le\mathfrak{m}} p^{\frac{2}{p^2-1}}\right) + (k+\frac{1}{2})\log(1-\frac{g_1}{k})}{\log(k-g_1)-1+\log z_1} - \tag{9.3.29}$$
$$\frac{(1.5\pi(\mathfrak{m}) - .5\ell - 1)\log k + \log\left(\mathfrak{n}_1^{-1}\mathfrak{n}_2\prod\limits_{p\le\mathfrak{m}} p^{.5+\frac{2}{p^2-1}}\right)}{\log(k-g_1)-1+\log z_1}$$

where

$$\mathfrak{n}(k,p) = \begin{cases} [\frac{\log(k-1)}{\log p}] & \text{if } [\frac{\log(k-1)}{\log p}] \text{ is even} \\ [\frac{\log(k-1)}{\log p}] - 1 & \text{if } [\frac{\log(k-1)}{\log p}] \text{ is odd,} \end{cases}$$

$$\ell = |\{p \le \mathfrak{m} : p|d\}|,\ \mathfrak{n}_0 = \prod_{\substack{p|d \\ p\le\mathfrak{m}}} p^{\frac{1}{p+1}},\ \mathfrak{n}_1 = \prod_{\substack{p|d \\ p\le\mathfrak{m}}} p^{\frac{p-1}{2(p+1)}} \text{ and } \mathfrak{n}_2 = \begin{cases} 2^{\frac{1}{6}} & \text{if } 2 \nmid d \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Since $|R| \geq t - g + 1 = k - g_1 + i_0$, we get

$$\prod_{b_i \in R} b_i \geq z_1^{k-g_1}(k-g_1)!. \tag{9.3.30}$$

Let

$$\vartheta_p = \text{ord}_p\left(\prod_{b_i \in R} b_i\right), \ \vartheta'_p = 1 + \text{ord}_p((k-1)!).$$

Let h be the positive integer such that $p^h \leq k-1 < p^{h+1}$ and $\epsilon = 1$ or 0 according as h is even or odd, respectively. Then

$$\vartheta'_p - 1 = \left[\frac{k-1}{p}\right] + \left[\frac{k-1}{p^2}\right] + \cdots + \left[\frac{k-1}{p^h}\right]. \tag{9.3.31}$$

Let $p \nmid d$. We show that

$$\vartheta_p - \vartheta'_p < -\frac{2k}{p^2-1}(1 - \frac{1}{p^{\mathfrak{n}(k,p)}}) + 1.5\mathfrak{n}(k,p) \tag{9.3.32}$$

$$< -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p} + .5 + \frac{2}{p^2-1} + \mathfrak{n}_3 \tag{9.3.33}$$

where $\mathfrak{n}_3 = \frac{1}{6}$ if $p = 2$ and 0 otherwise. We see that ϑ_p is the number of elements in $\{n + \gamma_1 d, n + \gamma_2 d, \ldots, n + \gamma_t d\}$ divisible by p to an odd power. For a positive integer s with $s \leq h$, let $0 \leq i_{p^s} < p^s$ be such that $p^s | n + i_{p^s} d$. Then we observe that p^s divides exactly $1 + \left[\frac{k-1-i_{p^s}}{p^s}\right]$ elements in $\{n, n+d, \ldots, n+(k-1)d\}$. After removing a term to which p appears to a maximal power, the number of remaining elements in $\{n, n+d, \ldots, n+(k-1)d\}$ divisible by p to an odd power is at most

$$\left[\frac{k-1-i_p}{p}\right] - \left[\frac{k-1-i_{p^2}}{p^2}\right] + \left[\frac{k-1-i_{p^3}}{p^3}\right] - \cdots + (-1)^{\epsilon}\left[\frac{k-1-i_{p^h}}{p^h}\right].$$

Since $\left[\frac{k}{p^s}\right] - 1 \leq \left[\frac{k-1-i_{p^s}}{p^s}\right] \leq \left[\frac{k-1}{p^s}\right]$, we obtain

$$\vartheta_p - 1 \leq \left[\frac{k-1}{p}\right] - \left[\frac{k}{p^2}\right] + \left[\frac{k-1}{p^3}\right] - \cdots + (-1)^{\epsilon}\left[\frac{k-1+\epsilon}{p^h}\right] + \frac{h-1+\epsilon}{2}.$$

This with (9.3.31) implies

$$\vartheta_p - \vartheta'_p \leq -\sum_{j=1}^{\frac{h-1+\epsilon}{2}}\left(\left[\frac{k-1}{p^{2j}}\right] + \left[\frac{k}{p^{2j}}\right]\right) + \frac{h-1+\epsilon}{2}. \tag{9.3.34}$$

Since $[\frac{k}{p^{2j}}] \geq [\frac{k-1}{p^{2j}}] \geq \frac{k-1}{p^{2j}} - 1 + \frac{1}{p^{2j}} = \frac{k}{p^{2j}} - 1$, we obtain

$$\vartheta_p - \vartheta'_p \leq -2k\sum_{j=1}^{\frac{h-1+\epsilon}{2}}\frac{1}{p^2} + 1.5(h-1+\epsilon)$$

giving (9.3.32) since $\mathfrak{n}(k,p) = h - 1 + \epsilon$. Further from (9.3.32), $k \leq p^{h+1}$ and $h < \frac{\log k}{\log p}$, we get

$$\vartheta_p - \vartheta'_p < -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p} + \frac{2p^{2-\epsilon}}{p^2-1} + 1.5(\epsilon - 1)$$

giving (9.3.33). For $p|d$, we get $\vartheta_p - \vartheta'_p = -1 - \text{ord}_p(k-1)!$ which together with Lemma 3.1.6 gives

$$\begin{aligned} \vartheta_p - \vartheta'_p &< -\frac{k}{p-1} + \frac{\log k}{\log p} + \frac{1}{p-1} \\ &< -\frac{2k}{p^2-1} + \frac{1.5\log k}{\log p} + .5 + \frac{2}{p^2-1} - \frac{k}{p+1} - \frac{.5\log k}{\log p} - \frac{p-1}{2(p+1)}. \end{aligned} \tag{9.3.35}$$

For $\mathfrak{m} > 1$, we have

$$\prod_{b_i \in R} b_i \ \Big| \ (k-1)! \left(\prod_{p \le k} p\right) \prod_{p \le \mathfrak{m}} p^{\vartheta_p - \vartheta'_p}.$$

Therefore from Lemma 3.1.2 (*iii*), (9.3.35), (9.3.32) and (9.3.33), we have

$$\prod_{b_i \in R} b_i < k! k^{-.5\ell - 1} \left(\mathfrak{n}_1^{-1} \prod_{p \le \mathfrak{m}} p^{1.5\mathfrak{n}(k,p)}\right) \left(\frac{\mathfrak{n}_0}{2.71851} \prod_{p \le \mathfrak{m}} p^{\frac{2}{p^2-1}(1 - \frac{1}{p^{\mathfrak{n}(k,p)}})}\right)^{-k} \tag{9.3.36}$$

and

$$\prod_{b_i \in R} b_i < k! k^{1.5\pi(\mathfrak{m}) - .5\ell - 1} \left(\mathfrak{n}_1^{-1} \mathfrak{n}_2 \prod_{p \le \mathfrak{m}} p^{.5 + \frac{2}{p^2-1}}\right) \left(\frac{\mathfrak{n}_0}{2.71851} \prod_{p \le \mathfrak{m}} p^{\frac{2}{p^2-1}}\right)^{-k}. \tag{9.3.37}$$

Comparing (9.3.36) and (9.3.37) with (9.3.30), we get

$$\frac{z_1^{g_1} k!}{(k-g_1)!} > k^{.5\ell + 1} \left(\mathfrak{n}_1^{-1} \prod_{p \le \mathfrak{m}} p^{1.5\mathfrak{n}(k,p)}\right)^{-1} \left(\frac{z_1 \mathfrak{n}_0}{2.71851} \prod_{p \le \mathfrak{m}} p^{\frac{2}{p^2-1}(1 - \frac{1}{p^{\mathfrak{n}(k,p)}})}\right)^{k} \tag{9.3.38}$$

and

$$\frac{z_1^{g_1} k!}{(k-g_1)!} > k^{-1.5\pi(\mathfrak{m}) + .5\ell + 1} \left(\mathfrak{n}_1^{-1} \mathfrak{n}_2 \prod_{p \le \mathfrak{m}} p^{.5 + \frac{2}{p^2-1}}\right)^{-1} \left(\frac{z_1 \mathfrak{n}_0}{2.71851} \prod_{p \le \mathfrak{m}} p^{\frac{2}{p^2-1}}\right)^{k}. \tag{9.3.39}$$

By Lemma 3.1.7, we have

$$\frac{z_1^{g_1} k!}{(k-g_1)!} < z_1^{g_1} e^{-g_1} (k-g_1)^{g_1} \left(\frac{k}{k-g_1}\right)^{k+\frac{1}{2}} = \left(\frac{z_1(k-g_1)}{e}\right)^{g_1} \left(1 - \frac{g_1}{k}\right)^{-k-\frac{1}{2}}.$$

This together with (9.3.38) and (9.3.39) imply the assertions (9.3.28) and (9.3.29), respectively. □

9.4. Lemmas for the lower bound for $n + (k-1)d$

We observe that $|S_1| \ge \frac{|T_1|}{2^{\omega(d)-\theta}}$ and $n + (k-1)d \ge |S_1|k^2$. We give lower bound for $|T_1|$. We have

LEMMA 9.4.1. *Let $k \ge 4$. Then*

$$|T_1| > t - \frac{(k-1)\log\,(k-1) - \sum_{p|d, p<k} \max\left(0, \frac{(k-1-p)\log p}{p-1} - \log(k-2)\right)}{\log\,(n + (k-1)d)} - \pi_d(k) - 1. \tag{9.4.1}$$

PROOF. The proof depends on an idea of Sylvester and Erdős and it is similar to [**63**, Lemma 3]. Since $|T_1| = t - |T|$, we may assume that $|T| > \pi_d(k)$. For a prime q with $q \le k$ and $q \nmid d$, let i_q be a term such that $\text{ord}_q(B_{i_q})$ is maximal. Let $T' = T \setminus \{i_q : q \le k, q \nmid d\}$. Thus $|T'| \ge |T| - \pi_d(k)$. Let $i \in T'$. Then $n + \gamma_i d = B_i$ and $\text{ord}_q(n + \gamma_i d) \le \text{ord}_q(\gamma_i - \gamma_{i_q})$ since $\gcd(n, d) = 1$. Therefore

$$\text{ord}_q(\prod_{i \in T'} (n + \gamma_i d)) \le \text{ord}_q((\gamma_{i_q})!(k - 1 - \gamma_{i_q})!) \le \text{ord}_q(k-1)!.$$

This, with $n + id \ge \frac{i}{k-1}(n + (k-1)d)$ for $i > 0$, gives

$$(|T'| - 1)! \left(\frac{n + (k-1)d}{k-1}\right)^{|T'|-1} < \prod_{i \in T'} (n + \gamma_i d) \le (k-1)! \varrho^{-1}$$

where $\varrho = \prod_{q|d} q^{\text{ord}_q(k-1)!}$. Therefore

$$\begin{aligned} &(|T| - \pi_d(k) - 1)\log(n + (k-1)d) \\ <&(|T'| - 1)\log(k-1) + \log((k-1)\cdots|T'|) - \log\psi \le (k-1)\log(k-1) - \log\varrho. \end{aligned}$$

Now the assertion (9.4.1) follows from Lemma 3.1.6. □

LEMMA 9.4.2. *Let $S \subseteq \{B_i : 1 \le i \le t\}$ and $\min\limits_{B_i \in S} B_i \ge U$. Let $h \ge 1$ and $P_1 < P_2 < \cdots < P_h$ be a subset of odd primes dividing d. Assume that*

$$|S| > Q\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_h-1}{2}\right) \tag{9.4.2}$$

where $Q \ge 1$ is an integer. Then

$$\max_{B_i \in S} B_i \ge 2^\delta Q P_1 \cdots P_h + U. \tag{9.4.3}$$

PROOF. For an odd $p|d$, we have from

$$\left(\frac{B_i}{p}\right) = \left(\frac{B_i Y_i^2}{p}\right) = \left(\frac{n}{p}\right)$$

that B_i belongs to at most $\frac{p-1}{2}$ distinct residue classes modulo p. If d is even, then B_i also belongs to a unique residue class modulo 2^δ. Hence, by Chinese remainder theorem, B_i belongs to at most $\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_j-1}{2}\right)$ distinct residue classes modulo $2^\delta P_1 \cdots P_j$ for each j, $1 \le j \le h$. Assume that (9.4.3) does not hold. Then

$$\max_{B_i \in S} A_i - (U-1) \le 2^\delta Q P_1 \cdots P_h.$$

Therefore

$$|S| \le \frac{2^\delta Q P_1 \cdots P_h}{2^\delta P_1 \cdots P_h}\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_h-1}{2}\right)$$

contradicting (9.4.2). □

COROLLARY 9.4.3. *Let $S \subseteq \{B_i : 1 \le i \le t\}$. Let $h \ge 1$ and $P_1 < P_2 < \cdots < P_h$ be a subset of odd primes dividing d. For $|S| > \left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_h-1}{2}\right)$, we have*

$$\max_{B_i \in S} B_i \ge \begin{cases} 2^\delta \rho(|S|-1)+1 & \text{if } h=1, 2|d \text{ or } 3|d \\ \frac{3}{4}2^{h+\delta}|S| & \text{if } 3\nmid d, h>1 \text{ if } 2|d \\ \frac{9}{8}2^{h+\delta}|S| & \text{if } 3|d, h>1. \end{cases} \tag{9.4.4}$$

PROOF. The assertion (9.4.4) with $h = 1, 2|d$ or $3|d$ follows by taking residue classes modulo 2^δ and 3. Thus we suppose $h \ge 2$ if $2|d$ or $3|d$. We have $|S| = Q\left(\frac{P_1-1}{2}\right) + \varepsilon$ with $Q \ge 1, 0 \le \varepsilon < \frac{P_1-1}{2}$ if $h = 1$ and $|S| = Q\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_h-1}{2}\right) + Q'\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right) + \varepsilon$ with $Q \ge 1, 0 \le Q' < \frac{P_h-1}{2}$ and $0 \le \varepsilon < \left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right)$ if $h > 1$. If $\varepsilon > 0$, then we take $Q_h = Q, Q'_h = Q', \varepsilon_h = \varepsilon$; if $\varepsilon = 0, Q' > 0$, we take $Q_h = Q, Q'_h = Q'-1, \varepsilon_h = \left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right)$. If $\varepsilon = 0, Q' = 0$, then $Q \ge 2$ and we take $Q_h = Q-1, Q'_h = \frac{P_h-1}{2}, \varepsilon_h = \left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right)$. We write

$$|S| = \begin{cases} Q_1\left(\frac{P_1-1}{2}\right) + \varepsilon_1 & \text{if } h=1 \\ Q_h\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_h-1}{2}\right) + Q'_h\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right) + \varepsilon_h & \text{if } h>1. \end{cases} \tag{9.4.5}$$

We arrange the elements of S in increasing order and let $S^1_{(h)} \subseteq S$ be the first ε_h elements. Further for $h > 1$, let $S^2_{(h)}$ consist of the first $Q'_h\left(\frac{P_1-1}{2}\right)\cdots\left(\frac{P_{h-1}-1}{2}\right) + \varepsilon_h$ elements of S. By taking modulo 2^δ and ρ, we get max $B_i \ge 2^\delta\rho(\varepsilon_h - 1) + 1$ for $B_i \in S^1_{(h)}$.

Let $h = 1$ and $\gcd(d, 6) = 1$. Then we see from Lemma 9.4.2 with $U = \varepsilon_1$, $h = 1$ and $Q = Q_1$ that

$$\max_{B_i \in S} B_i \ge Q_1 P_1 + \varepsilon_1.$$

Now we observe from $\varepsilon_1 \le \frac{P_1-1}{2}$ and (9.4.5) that (9.4.4) is valid.

Thus $h > 1$. If $Q' > 0$, we apply Lemma 9.4.2 with $S = S^2_{(h)}$, $U = 2^\delta \rho(\varepsilon_h - 1) + 1$, $Q = Q'_h$ to derive

$$\max_{B_i \in S^2_{(h)}} B_i \geq 2^\delta Q'_h P_1 P_2 \cdots P_{h-1} + 2^\delta \rho(\varepsilon_h - 1) + 1 := U_1.$$

The same assertion is also valid when $Q' = 0$. Now we apply Lemma 9.4.2 in S with $U = U_1, Q = Q_h$ to get

$$\max_{B_i \in S} B_i \geq 2^\delta Q_h P_1 P_2 \cdots P_h + 2^\delta Q'_h P_1 P_2 \cdots P_{h-1} + 2^\delta \rho(\varepsilon_h - 1) + 1 := U'.$$

Let $3 \nmid d$. Since $\varepsilon_h \leq \left(\frac{P_1-1}{2}\right) \cdots \left(\frac{P_{h-1}-1}{2}\right)$ and $(P_{h-1} - 1)(P_h - 1) \leq P_{h-1}P_h - 2P_{h-1}$, for deriving (9.4.4), it suffices to prove

$$Q_h P_1 \cdots P_h + Q'_h P_1 \cdots P_{h-1} \geq \frac{3}{4} \left\{ Q_h P_1 \cdots P_h + (2Q'_h + 2 - 2Q_h) P_1 \cdots P_{h-1} \right\}.$$

This follows from

$$Q_h P_h + 6(Q_h - 1) - 2Q'_h \geq 0 \tag{9.4.6}$$

which is true since $Q_h \geq 1$ and $Q'_h \leq \frac{P_h - 1}{2}$.

Thus $3|d$. Then $P_1 = 3$. Let $h = 2$. Then $\varepsilon = 1$ since $1 \leq \varepsilon \leq \frac{P_1-1}{2}$ and it suffices to prove

$$Q_h P_2 + Q'_h \geq \frac{3}{4} \left\{ Q_h (P_2 - 1) + 2Q'_h + 2 \right\}$$

From $Q_h \geq 1, Q'_h \leq \frac{P_2-1}{2}$, we see that $Q_h P_2 + 3(Q_h - 2) - 2Q'_h \geq 0$ if either $Q_h > 1$ or $Q'_h < \frac{P_2-1}{2}$. Therefore we may suppose that $Q_h = 1$ and $Q'_h < \frac{P_2-1}{2}$ implying $|S| = 2(\frac{P_2-1}{2}) + 1$. Now we get from Lemma 9.4.2 that Max $B_i \geq 2^\delta \cdot 3 \cdot 2P_2 + 1$ for $B_i \in S$. Now the assertion follows since $|S| = P_2| + 1$ and $P_2 \geq 5$. Hence $h > 2$. To derive (9.4.4), it is enough to prove

$$Q_h P_2 \cdots P_h + Q'_h P_2 \cdots P_{h-1} \geq \frac{3}{4} \left\{ Q_h P_2 \cdots P_h + (2Q'_h + 2 - 2Q_h) P_2 \cdots P_{h-1} \right\}.$$

As in $3 \nmid d$, it follows from (9.4.6) which is true since $Q_h \geq 1$ and $Q'_h \leq \frac{P_h-1}{2}$. □

Corollary 9.4.4. *We have* $\lambda_1 < \frac{2}{3}\mathfrak{q}_1$ *if* $2 \nmid d, 3 \nmid d$ *and* $\lambda_1 < \frac{\mathfrak{q}_1}{\rho 2^\delta} + 1$ *otherwise. For* $h \geq 2$, *we have*

$$\lambda_h < \begin{cases} \frac{\mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_h}{3 \cdot 2^{h-2}} & \text{if } 2 \nmid d, 3 \nmid d \\ \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{9 \cdot 2^{h-3}} & \text{if } 2 \nmid d, 3|d \\ \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{3 \cdot 2^{\delta+h-3}} & \text{if } 2|d, 3 \nmid d \\ \min(\frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{3 \cdot 2^\delta} + 1, \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{9 \cdot 2^{h-2}}) & \text{if } 6|d. \end{cases}$$

Proof. Let $2 \nmid d$ and $3 \nmid d$. If $\lambda_h \geq \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_r}{3 \cdot 2^{h-2}}$, then $\lambda_h > \frac{\mathfrak{q}_1 - 1}{2} \cdots \frac{\mathfrak{q}_h - 1}{2} \geq \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_h - 1}{2}$ giving $\mathfrak{q}_1 \cdots \mathfrak{q}_h > \max\limits_{B_i \in \mathcal{A}_h} B_i \geq \frac{3}{4} 2^h \lambda_h$ by (9.4.4) with $S = \mathcal{A}_h$. This is a contradiction.

Let $2|d$ or $3|d$. Then we derive from Chinese remainder theorem that $\lambda_h < \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{\rho 2^\delta} + 1$. Thus we may suppose that $h \geq 2$. Further we may also assume that $h \geq \delta + 1$ when $6|d$.

Let $2 \nmid d$ and $3|d$. Suppose $\lambda_h \geq \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{9 \cdot 2^{h-3}}$. Then $\mathfrak{q}_1 \geq \mathfrak{p}_1 = 3$ implying $\lambda_h > \frac{\mathfrak{q}_2 - 1}{2} \cdots \frac{\mathfrak{q}_h - 1}{2} \geq \frac{\mathfrak{p}_1 - 1}{2} \frac{\mathfrak{p}_2 - 1}{2} \cdots \frac{\mathfrak{p}_h - 1}{2}$. Therefore $\mathfrak{q}_1 \cdots \mathfrak{q}_h > \frac{9}{4} 2^{h-1} \lambda_h$ by (9.4.4) with $S = \mathcal{A}_h$. This is a contradiction.

Let $2|d$ and $3 \nmid d$. Suppose $\lambda_h \geq \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{3 \cdot 2^{\delta+h-3}}$. Then $\mathfrak{q}_h \geq 7$ since $h \geq 2$ implying $\mathfrak{q}' := \max(\mathfrak{q}_h, 2^\delta) \geq 7$ implying

$$\lambda_h \geq \frac{2^{h-1}\mathfrak{q}'}{3 \cdot 2^{\delta+h-3}} \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_{h-1} - 1}{2} \geq \frac{\mathfrak{q}'}{6} \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_{h-1} - 1}{2} > \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_{h-1} - 1}{2}.$$

Now we apply (9.4.4) with $S = \mathcal{A}_h$ to get a contradiction.

Let $6|d$. Suppose $\lambda_h \geq \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_h}{9 \cdot 2^{h-2}}$. Let $2||d$ or $4||d$. Then $\lambda_h > \frac{\mathfrak{q}_2-1}{2} \cdots \frac{\mathfrak{q}_{h-1}-1}{2} \geq \frac{\mathfrak{p}_1-1}{2}\frac{\mathfrak{p}_2-1}{2} \cdots \frac{\mathfrak{p}_{h-2}-1}{2}$ since $\mathfrak{q}_1\mathfrak{q}_h \geq 9$ and $\mathfrak{p}_1 = 3$. Now we apply (9.4.4) with $S = \mathcal{A}_h$ to get a contradiction. Thus it remains to consider $8|d$. Then $\lambda_h > \frac{\mathfrak{q}_2-1}{2} \cdots \frac{\mathfrak{q}_{h-1}-1}{2} \geq \frac{\mathfrak{p}_1-1}{2}\frac{\mathfrak{p}_2-1}{2} \cdots \frac{\mathfrak{p}_{h-1}-1}{2}$ since

$$\lambda_h \geq \frac{2^{h-2}\mathfrak{q}_1\mathfrak{q}'}{9 \cdot 2^{h-2}} \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_{h-2} - 1}{2} > \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_{h-2} - 1}{2}.$$

where $\mathfrak{q}' := \max(\mathfrak{q}_h, 8)$. Now we apply (9.4.4) with $S = \mathcal{A}_h$ to get a contradiction. □

Let t_ν denote the ν-th odd squarefree positive integer. We recall here s_ν is the ν-th squarefree positive integer. The next lemma gives a bound for s_ν and t_ν.

Lemma 9.4.5. *We have*

$$s_i \geq 1.6i \quad for \quad i \geq 78 \tag{9.4.7}$$

and

$$t_i \geq 2.4i \quad for \quad i \geq 51. \tag{9.4.8}$$

Further we have

$$\prod_{i=1}^{l} s_i \geq (1.6)^l l! \quad for \quad l \geq 286 \tag{9.4.9}$$

and

$$\prod_{i=1}^{l} t_i \geq (2.4)^l l! \quad for \quad l \geq 200. \tag{9.4.10}$$

Proof. The proof is similar to that of [**63**, (6.9)]. For (9.4.7) and (9.4.8), we check that $s_i \geq 1.6i$ for $78 \leq i \leq 286$ and $t_i \geq 2.4i$ for $51 \leq i \leq 132$, respectively. Further we observe that in a given set of 144 consecutive integers, there are at most 90 squarefree integers and at most 60 odd squarefree integers by deleting multiples of $4, 9, 25, 49, 121$ and $2, 9, 25, 49$, respectively. Then we continue as in the proof of [**63**, (6.9)] to get (9.4.7) and (9.4.8). Further we check that (9.4.9) holds at $l = 286$ and (9.4.10) holds at $l = 200$. Then we use (9.4.7) and (9.4.8) to obtain (9.4.9) and (9.4.10), respectively. □

Lemma 9.4.6. *Let $X > 1$ be a positive integer. Then*

$$\sum_{i=1}^{X-1} 2^{\omega(i)} \leq \varphi(X) X \log X \tag{9.4.11}$$

where

$$\varphi := \varphi(X) = \begin{cases} 1 & if\ X = 1 \\ \dfrac{\sum\limits_{i=1}^{X-1} 2^{\omega(i)}}{X\ \log X} & if\ 1 < X < 248 \\ 0.75 & if\ X \geq 248. \end{cases} \tag{9.4.12}$$

Proof. We check that (9.4.11) holds for $1 < X < 11500$. Thus we may assume $X \geq 11500$. Let s_j be the largest squarefree integer $\leq X$. Then $i \geq 78$ and hence by Lemma 9.4.5, we have $1.6j \leq s_j \leq X$ so that $j \leq \left[\frac{X}{1.6}\right]$. We have $2^{\omega(i)} = \sum_{e|i} |\mu(e)|$. Therefore

$$\sum_{i=1}^{X-1} 2^{\omega(i)} = \sum_{i=1}^{X-1} \sum_{e|i} |\mu(e)| \leq \sum_{1 \leq e < X} \left[\frac{X-1}{e}\right] |\mu(e)| \leq (X-1) \sum_{1 \leq e < X} \frac{|\mu(e)|}{e} \leq X \sum_{i=1}^{\left[\frac{X}{1.6}\right]} \frac{1}{s_i}.$$

We check that there are 6990 squarefree integers upto 11500. By using (9.4.7), we have

$$\begin{aligned}\sum_{i=1}^{X-1}2^{\omega(i)} &\le X\left\{\sum_{i=1}^{6990}\frac{1}{s_i}-\frac{1}{1.6}\sum_{i=1}^{6990}\frac{1}{i}+\frac{1}{1.6}\sum_{i=1}^{[\frac{X}{1.6}]}\frac{1}{i}\right\}\\ &\le X\left\{\sum_{i=1}^{6990}\frac{1}{s_i}-\frac{1}{1.6}\sum_{i=1}^{6990}\frac{1}{i}+\frac{1}{1.6}\left(1+\log\frac{X}{1.6}\right)\right\}\\ &\le \frac{3}{4}X\log X\left\{\frac{4}{3}\frac{1.1658}{\log X}+\frac{4}{3}\frac{1}{1.6}\right\}\end{aligned}$$

implying (9.4.11). □

LEMMA 9.4.7. *Let $c>0$ be such that $c2^{\omega(d)-3}>1$, $\mu\ge 2$ and*

$$\mathfrak{C}_\mu=\{B_i : i\in T_1,\ \nu(B_i)=\mu,\ B_i>\frac{\rho 2^\delta k}{3c2^{\omega(d)}}\}.$$

Then

$$\mathfrak{C}:=\sum_{\mu\ge 2}\frac{\mu(\mu-1)}{2}|\mathfrak{C}_\mu|\le\frac{c}{8}\varphi(c2^{\omega(d)-3})2^{\omega(d)}(2^{\omega(d)-\theta}-1)(\log c2^{\omega(d)-3}). \tag{9.4.13}$$

PROOF. Let $i_1>i_2\cdots>i_\mu$ be such that $B_{i_1}=B_{i_2}=\cdots=B_{i_\mu}$. These give rise to $\frac{\mu(\mu-1)}{2}$ pairs of $(i,j), i>j$ with $B_i=B_j$. Therefore the total number of pairs (i,j) with $i,j\in T_1, i>j$ and $B_i=B_j>\frac{\rho 2^\delta k}{3c2^{\omega(d)}}$ is $\mathfrak{C}$.

We know that there is a unique partition of d corresponding to each pair $(i,j), i>j$ such that $B_i=B_j$. Hence by Box Principle, there exists at least $\frac{\mathfrak{C}}{2^{\omega(d)-\theta}-1}$ pairs of $(i,j), i>j$ with $B_i=B_j$ and a partition (d_1,d_2) of d corresponding to these pairs. For every such pair (i,j), we write $Y_i-Y_j=d_1r_{ij},\ Y_i+Y_j=d_2s_{ij}$. Then $\gcd(Y_i-Y_j,Y_i+Y_j)=2$ and $24|(Y_i^2-Y_j^2)$. Hence $\frac{24}{\rho 2^\delta}|r_{ij}s_{ij}$. Let $r'_{ij}=\frac{r_{ij}}{\gcd(r_{ij},\frac{24}{\rho 2^\delta})}$ and $s'_{ij}=\frac{s_{ij}}{\gcd(s_{ij},\frac{24}{\rho 2^\delta})}$ so that $r'_{ij}s'_{ij}=\frac{\rho 2^\delta}{24}r_{ij}s_{ij}$. Then

$$r'_{ij}s'_{ij}=\frac{\rho 2^\delta}{24}r_{ij}s_{ij}=\frac{\rho 2^\delta}{24}\frac{Y_i^2-Y_j^2}{d}=\frac{\rho 2^\delta}{24}\frac{i-j}{B_i}<\frac{\rho 2^\delta}{24}\frac{k}{B_i}<c2^{\omega(d)-3}$$

since $B_i>\frac{\rho 2^\delta k}{3c2^{\omega(d)}}$. There are at most $\sum_{i=1}^{c2^{\omega(d)-3}-1}2^{\omega(i)}$ possible pairs of (r'_{ij},s'_{ij}), and hence an equal number of possible pairs of (r_{ij},s_{ij}). By Lemma 9.4.6, we estimate

$$\sum_{i=1}^{c2^{\omega(d)-3}-1}2^{\omega(i)}\le\varphi(c2^{\omega(d)-3})c2^{\omega(d)-3}(\log c2^{\omega(d)-3}).$$

Thus if we have

$$\frac{\mathfrak{C}}{2^{\omega(d)-\theta}-1}>\varphi(c2^{\omega(d)-3})c2^{\omega(d)-3}(\log c2^{\omega(d)-3}),$$

then there exist distinct pairs $(i,j)\ne(g,h), i>j, g>h$ with $B_i=B_j, B_g=B_h$ such that $r_{ij}=r_{gh}, s_{ij}=s_{gh}$ giving

$$Y_i-Y_j=d_1r_{ij}=Y_g-Y_h \text{ and } Y_i+Y_j=d_2s_{ij}=Y_g+Y_h.$$

Thus $Y_i=Y_g, Y_j=Y_h$ implying $(i,j)=(g,h)$, a contradiction. Hence

$$\frac{\mathfrak{C}}{2^{\omega(d)-\theta}-1}\le\varphi(c2^{\omega(d)-3})c2^{\omega(d)-3}(\log c2^{\omega(d)-3})$$

implying (9.4.13). □

9.5. Estimates on the general upper bound of $\nu(a)$ for $a \in R$

In this section, we give upper bound of $\nu(a)$ with $a \in R$ which are independent of $\omega(d)$.

Let $\bar{f}(x) = \lceil x \rceil - [\frac{\lceil x \rceil}{4}]$ for $x > 0$ and $\mathcal{K}_a = \frac{k}{a2^{3-\delta}}$ for $a \in R$. We have

LEMMA 9.5.1. *Let $a \in R$ and μ be a positive integer. Let p, q be distinct odd primes.*
(i) Let $f_0(k,a,\delta) = \bar{f}(\mathcal{K}_a)$,

$$f_1(k,a,p,\mu,\delta) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}}) + \bar{f}(\frac{\mathcal{K}_a}{p^{2\mu}})$$

and

$$f_2(k,a,p,q,\mu,\delta) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\left(\frac{q-1}{2}\bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}q}) + \bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}q^2})\right) + \bar{f}(\frac{\mathcal{K}_a}{p^{2\mu}}).$$

Then

$$\nu_o(a) \le \begin{cases} f_0(k,a,\delta) \\ f_1(k,a,p,\mu,\delta) & \text{if } p \nmid d \\ f_2(k,a,p,q,\mu,\delta) & \text{if } p \nmid d, q \nmid d. \end{cases} \tag{9.5.1}$$

(ii) Let d be odd. Let

$$g_0(k,a,\mu) = \sum_{l=1}^{\mu-1}\bar{f}(\frac{\mathcal{K}_a}{2^{2l}}) + \bar{f}(\frac{k}{a2^{2\mu}}),$$

$$g_1(k,a,p,\mu) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j p^{2l+1}}) + \sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j p^{2\mu}})$$

and

$$g_2(k,a,p,q,\mu) = \frac{p-1}{2}\sum_{l=0}^{\mu-1}\sum_{j=1}^{2}\left(\frac{q-1}{2}\bar{f}(\frac{\mathcal{K}_a}{2^j p^{2l+1}q}) + \bar{f}(\frac{\mathcal{K}_a}{2^j p^{2l+1}q^2})\right) + \sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j p^{2\mu}}).$$

Then

$$\nu_e(a) \le \begin{cases} g_0(k,a,\mu) \\ g_1(k,a,p,\mu) & \text{if } p \nmid d \\ g_2(k,a,p,q,\mu) & \text{if } p \nmid d, q \nmid d. \end{cases} \tag{9.5.2}$$

PROOF. Let $\mathcal{I} \subseteq \{i : a_i = a\}$ and $\tau|(i-j)$ whenever $i, j \in \mathcal{I}$. Let τ' be the lcm of all τ_1 such that $\tau_1|(i-j)$ whenever $i, j \in \mathcal{I}$. Then $\tau|\tau'$ and $a|\tau'$ since $a|(i-j)$ whenever $i, j \in \mathcal{I}$. Let $i_0 = \min_{i \in \mathcal{I}} i$, $N = \frac{n+i_0 d}{a}$ and $D = \frac{\tau'}{a}d$. Then we see that ax_i^2 with $i \in \mathcal{I}$ come from the squares in the set $\{N, N+D, \cdots, N+(\lceil\frac{k-i_0}{\tau}\rceil - 1)D\}$. Dividing this set into consecutive intervals of length 4 and using Euler's result, we see that there are at most $\lceil\frac{k-i_0}{\tau'}\rceil - [\frac{\lceil\frac{k-i_0}{\tau'}\rceil}{4}] \le \lceil\frac{k}{\tau'}\rceil - [\frac{\lceil\frac{k}{\tau'}\rceil}{4}] = \bar{f}(\frac{k}{\tau'})$ of them which can be squares. Hence $|\mathcal{I}| \le \bar{f}(\frac{k}{\tau'}) \le \bar{f}(\frac{k}{\tau})$ since $\tau|\tau'$.

Let $\mathcal{I}^o = \{i : a_i = a, 2 \nmid x_i\}$ and $\mathcal{I}^e = \{i : a_i = a, 2|x_i\}$. Then $\nu_o(a) = |\mathcal{I}^o|$ and $\nu_e(a) = |\mathcal{I}^e|$.

First we prove (9.5.1). For $i, j \in \mathcal{I}^o$, we observe from $x_i^2, x_j^2 \equiv 1 (\text{mod } 8)$ and $(i-j)d = a(x_i^2 - x_j^2)$ that $a2^{3-\delta}|(i-j)$. Therefore $|\mathcal{I}^o| \le \bar{f}(\mathcal{K}_a) = f_0(k,a,\delta)$.

For a prime p', let

$$\mathfrak{Q}_{p'} = \{m : 1 \le m < p', \left(\frac{m}{p'}\right) = 1\}.$$

Let $p \nmid d$. Let

$$\mathcal{I}_l^o = \{i \in \mathcal{I}^o : p^l || x_i\} \text{ for } 0 \le l < \mu \text{ and } \mathcal{I}_\mu^o = \{i \in \mathcal{I}^o : p^\mu | x_i\}.$$

Then $a2^{3-\delta}p^{2\mu}|(i-j)$ whenever $i, j \in \mathcal{I}^o_\mu$ giving $|\mathcal{I}^o_\mu| \le \bar{f}(\frac{\mathcal{K}_a}{p^{2\mu}})$. For each $l, 0 \le l < \mu$ and for each $m \in \mathfrak{Q}_p$, let

$$\mathcal{I}^o_{lm} = \{i \in \mathcal{I}^o_l : (\frac{x_i}{p^l})^2 \equiv m (\text{mod } p)\}.$$

Then $a2^{3-\delta}p^{2l+1}|(i-j)$ whenever $i, j \in \mathcal{I}^o_{lm}$ giving $|\mathcal{I}^o_{lm}| \le \bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}})$. Therefore $|\mathcal{I}^o_l| = \sum_{m \in \mathfrak{Q}_p} |\mathcal{I}^o_{lm}| \le \frac{p-1}{2}\bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}})$. Hence $|\mathcal{I}^o| = |\mathcal{I}^o_\mu| + \sum_{l=0}^{\mu-1} |\mathcal{I}^o_l| \le f_1(k, a, p, \mu, \delta)$.

Thus we may assume that $p \nmid d$ and $q \nmid d$. For each l with $0 \le l < \mu$, $m \in \mathfrak{Q}_p$ and for each $u \in \mathfrak{Q}_q$, let

$$\mathcal{I}^o_{lmu} = \{i \in \mathcal{I}^o_{lm} : x_i^2 \equiv u (\text{mod } q)\} \text{ and } \mathcal{I}^o_{lm0} = \{i \in \mathcal{I}^o_{lm} : q|x_i)\}.$$

Then $a2^{3-\delta}p^{2l+1}q|(i-j)$ for $i, j \in \mathcal{I}^o_{lmu}$ and $a2^{3-\delta}p^{2l+1}q^2|(i-j)$ for $i, j \in \mathcal{I}^o_{lm0}$ implying $|\mathcal{I}^o_{lmu}| \le \bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}q})$ for $u \in \mathfrak{Q}_q$ and $|\mathcal{I}^o_{lm0}| \le \bar{f}(\frac{\mathcal{K}_a}{p^{2l+1}q^2})$. Now the assertion $\nu_o(a) \le f_2(k, a, p, q, \mu, \delta)$ follows from

$$|\mathcal{I}^o_{lm}| \le |\mathcal{I}^o_{lm0}| + \sum_{u \in \mathfrak{Q}_q} |\mathcal{I}^o_{lmu}|, |\mathcal{I}^o_l| = \sum_{m \in \mathfrak{Q}_p} |\mathcal{I}^o_{lm}|, \text{ and } |\mathcal{I}^o| = |\mathcal{I}^o_\mu| + \sum_{l=0}^{\mu-1} |\mathcal{I}^o_l|.$$

Now we turn to the proof of (9.5.2). Let

$$\mathcal{I}^{el} = \{i \in \mathcal{I}^e : 2^l || x_i\} \text{ for } 1 \le l < \mu \text{ and } \mathcal{I}^{e\mu} = \{i \in \mathcal{I}^e : 2^\mu | x_i\}.$$

Since $\frac{x_i}{2^l}$ is odd, we get $a2^{2l+3}|(i-j)$ whenever $i, j \in \mathcal{I}^{el}$ implying $|\mathcal{I}^{el}| \le \bar{f}(\frac{\mathcal{K}_a}{2^{2l}})$ for $0 \le l < \mu$. Further $a2^{2\mu}|(i-j)$ for $i, j \in \mathcal{I}^{e\mu}$ giving $|\mathcal{I}^{e\mu}| \le \bar{f}(\frac{k}{a2^{2\mu}})$. Now the assertion $\nu_e(a) \le g_0(k, a, \mu)$ from $|\mathcal{I}^e| = |\mathcal{I}^{e\mu}| + \sum_{l<\mu} |\mathcal{I}^{el}|$.

For the remaining proofs of (9.5.2), we consider $\mathcal{I}^{e1} = \{i \in \mathcal{I}^e : 2||x_i\}$, $\mathcal{I}^{e2} = \{i \in \mathcal{I}^e : 4|x_i\}$ so that $|\mathcal{I}^e| = |\mathcal{I}^{e1}| + |\mathcal{I}^{e2}|$. Then $32a|(i-j)$ for $i, j \in \mathcal{I}^{e1}$ and $16a|(i-j)$ for $i, j \in \mathcal{I}^{e2}$. We now continue the proof as in that of (9.5.1) with $\mathcal{I}^{e1}, \mathcal{I}^{e2}$ in place of $\mathcal{I}^o$ to get $\nu_e(a) \le g_1(k, a, p, \mu)$ when $p \nmid d$ and $\nu_e(a) \le g_2(k, a, p, q, \mu)$ when $p \nmid d, q \nmid d$. □

From Lemma 9.5.1, we derive

Lemma 9.5.2. *For $a \in R$, let*

$$f_3(k, a, \delta) = \begin{cases} 1 & \text{if } k \le a2^{3-\delta} \\ \bar{f}(\mathcal{K}_a) & \text{if } k > a2^{3-\delta}, 3|d, 5|d \\ \bar{f}(\frac{\mathcal{K}_a}{3}) + \bar{f}(\frac{\mathcal{K}_a}{9}) & \text{if } k > a2^{3-\delta}, 3 \nmid d, 5|d \\ \bar{f}(\mathcal{K}_a) & \text{if } a2^{3-\delta} < k \le 2a2^{3-\delta}, 3|d, 5 \nmid d \\ 2\bar{f}(\frac{\mathcal{K}_a}{5}) + \bar{f}(\frac{\mathcal{K}_a}{25}) & \text{if } k > 2a2^{3-\delta}, 3|d, 5 \nmid d \\ \bar{f}(\frac{\mathcal{K}_a}{3}) + \bar{f}(\frac{\mathcal{K}_a}{9}) & \text{if } a2^{3-\delta} < k \le 24a2^{3-\delta}, 3 \nmid d, 5 \nmid d \\ 2\left(\bar{f}(\frac{\mathcal{K}_a}{15}) + \bar{f}(\frac{\mathcal{K}_a}{135})\right) + & \\ \bar{f}(\frac{\mathcal{K}_a}{75}) + \bar{f}(\frac{\mathcal{K}_a}{675}) + \bar{f}(\frac{\mathcal{K}_a}{81}) & \text{if } 24a2^{3-\delta} < k \le 324a2^{3-\delta}, 3 \nmid d, 5 \nmid d \\ 2\left(\bar{f}(\frac{\mathcal{K}_a}{15}) + \bar{f}(\frac{\mathcal{K}_a}{135}) + \bar{f}(\frac{\mathcal{K}_a}{1215})\right) + & \\ \bar{f}(\frac{\mathcal{K}_a}{75}) + \bar{f}(\frac{\mathcal{K}_a}{675}) + \bar{f}(\frac{\mathcal{K}_a}{6075}) + \bar{f}(\frac{\mathcal{K}_a}{729}) & \text{if } k > 324a2^{3-\delta}, 3 \nmid d, 5 \nmid d \end{cases}$$

and

$$g_3(k,a)=\begin{cases}1 & \text{if } k\le 4a\\ \sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j}) & \text{if } 4a<k\le 32a\\ \sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j}) & k>32a, 3|d, 5|d\\ \sum_{j=1}^{2}\big(\bar{f}(\frac{\mathcal{K}_a}{2\cdot 3^j})+\bar{f}(\frac{\mathcal{K}_a}{4\cdot 3^j})\big) & \text{if } k>32a, 3\nmid d, 5|d\\ \sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j}) & 32a<k\le 64a, 3|d, 5\nmid d\\ 2\sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j\cdot 5})+\sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j\cdot 25}) & \text{if } k>64a, 3|d, 5\nmid d\\ \sum_{j=1}^{2}\sum_{l=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j\cdot 3^l}) & \text{if } 32a<k\le 576a, 3\nmid d, 5\nmid d\\ 2\sum_{j=1}^{2}\sum_{l=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j\cdot 3^{2l-1}\cdot 5})+ & \\ \sum_{j=1}^{2}\sum_{l=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j\cdot 3^{2l-1}\cdot 25})+\sum_{j=1}^{2}\bar{f}(\frac{\mathcal{K}_a}{2^j\cdot 81}) & \text{if } k>576a, 3\nmid d, 5\nmid d.\end{cases}$$

Then for $a\in R$, we have

$$\nu_o(a)\le f_3(k,a,\delta),\ \ \nu_e(a)\le g_3(k,a)$$

and

$$\nu(a)\le F_0(k,a,\delta):=\begin{cases}1 & \text{if } k\le a\\ f_3(k,a,\delta) & \text{if } k>a \text{ and } d \text{ even}\\ f_3(k,a,0)+g_3(k,a) & \text{if } k>a \text{ and } d \text{ odd.}\end{cases}$$

Proof. Since $a|(i-j)$ whenever $a_i=a_j=a$, we get $\nu(a)\le 1$, $\nu_o(a)\le 1$, $\nu_e(a)\le 1$ for $k\le a$. In fact $\nu_o(a)\le 1$ for $k\le a2^{3-\delta}$ and $\nu_e(a)\le 1$ for $k\le 4a$. Thus we suppose that $k>a$. We have $\nu(a)=\nu_o(a)+\nu_e(a)$. It suffices to show $\nu_o(a)\le f_3(k,a,\delta)$ for $k>a2^{3-\delta}$ and $\nu_e(a)\le g_3(k,a)$ for $k>4a$ since $\nu_e(a)=0$ for d even. From (9.5.1), we get the assertion $\nu_o(a)\le f_3(k,a,\delta)$ for $k>a2^{3-\delta}$ since

$$\nu_o(a)\le\begin{cases}f_0(k,a,\delta) & \text{if } 15|d\\ f_1(k,a,3,1,\delta) & \text{if } 3\nmid d, 5|d\\ \min(f_0(k,a,\delta), f_1(k,a,5,1,\delta)) & \text{if } 3|d, 5\nmid d\\ \min(f_1(k,a,3,1,\delta), f_2(k,a,3,5,2,\delta), & \\ \ f_2(k,a,3,5,3,\delta)) & \text{if } 3\nmid d, 5\nmid d.\end{cases}$$

The assertion $\nu_e(a)\le g_3(k,a)$ for $k>4a$ follows from (9.5.2) since $\nu_e(a)\le g_0(k,a,2)$ for $4a<k\le 32a$ and

$$\nu_e(a)\le\begin{cases}g_0(k,a,2) & \text{if } 15|d\\ g_1(k,a,3,1)) & \text{if } 3\nmid d, 5|d\\ \min(g_0(k,a,2), g_1(k,a,5,1)) & \text{if } 3|d, 5\nmid d\\ \min(g_1(k,a,3,1), g_2(k,a,3,5,2)) & \text{if } 3\nmid d, 5\nmid d\end{cases}$$

for $k>32a$. □

We observe that there are $\frac{p-1}{2}$ distinct quadratic residues and $\frac{p-1}{2}$ distinct quadratic non-residue modulo an odd prime p. The next lemma follows easily from this fact.

Lemma 9.5.3. *Assume* (2.1.1) *holds. Let k be an odd prime. Suppose that $k\nmid d$. Then $\nu(a)\le \frac{k-1}{2}$ for any $a\in R$.*

CHAPTER 10

Extensions of a result of Euler: Proof of Theorems 2.1.1, 2.2.1 and 2.2.2

10.1. Introduction

For the convenience of the proofs, we consider Theorems 2.2.1 and 2.2.2 together. Therefore we formulate

Theorem 10.1.1.

Let $d > 1, P(b) \leq k$ and $5 \leq k \leq 100$. Suppose that $k \neq 5$ if $P(b) = k$. Then (2.1.1) *does not hold except for the* $(a_0, a_1, \cdots, a_{k-1})$ *among* (2.2.2), (2.2.3) *and their mirror images.*

It is clear that Theorem 10.1.1 implies Theorems 2.2.1 and 2.2.2. In fact the proof of Theorem 10.1.1 provides a method for solving (2.1.1) for any given value of k. We have restricted k up to 100 for keeping the computational load under control. We begin by proving the assertion for $k = 5$.

10.2. The case $k = 5$

Let $k = 5$. We show that (2.1.1) with $P(b) < k$ does not hold.

Assume that $n(n+d)(n+2d)(n+3d)(n+4d) = by^2$ where $b \in \{1, 2, 3, 6\}$. Then

$$(n+2d)^2\{(n+2d)^2 - d^2\}\{(n+2d)^2 - 4d^2\} = b'y'^2$$

where $(n+2d)by^2 = b'y'^2, b'$ is the squarefree part of $b(n+2d)$ and further $b' \in \{1, 2, 3, 6\}$. Multiplying both sides by $\frac{b'^3}{d^6}$ and putting $X = b'\frac{(n+2d)^2}{d^2}, Y = \frac{b'^2y'}{d^3}$, we obtain the elliptic equation

$$Y^2 = X(X - b')(X - 4b') = X^3 - 5b'X^2 + 4b'^2X.$$

For $b' \in \{1, 2, 3, 6\}$, we check using *MAGMA* that the above curves have rank 0. Further the torsion points are given by

$$\begin{aligned} b' = 1 &: (X, Y) = (0, 0), (1, 0), (4, 0), \\ b' = 2 &: (X, Y) = (0, 0), (2, 0), (8, 0), \\ b' = 3 &: (X, Y) = (0, 0), (3, 0), (12, 0), \\ b' = 6 &: (X, Y) = (0, 0), (6, 0), (24, 0). \end{aligned}$$

We observe from $Y > 0$ that the above torsion points do not give any solution for (2.1.1). □

From now on, we may suppose throughout this chapter that $k > 5$.

10.3. A Covering Lemma

In this section, we give a lemma central to the proof of Theorem 10.1.1.

Let q_1, q_2 be distinct primes and

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

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

Lemma 10.3.1. *We have*

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

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

$$\mathfrak{i}(\mathcal{P}) = |\{p \in \mathcal{P} : p \text{ divides } a_i\}|. \tag{10.3.1}$$

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

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

Lemma 10.3.2. *Let $\mathcal{P}_0$ be a set of primes. Let p_1, p_2 be primes such that* $\gcd(p_1 p_2, d) = 1$. *Let $(i_1, i_2) = (i_{p_1}, i_{p_2}), \mathcal{I} \subseteq [0, k) \cap \mathbb{Z}$ and $\mathcal{I}' = \mathcal{I}(p_1, p_2)$ be such that $\mathfrak{i}(\mathcal{P}_0 \cap \Lambda(p_1, p_2))$ is even for each $i \in \mathcal{I}'$. Define*

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

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

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

or

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

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

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

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

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

$$\mathcal{L} := \{i \in \mathcal{I}' : \left(\frac{a_i}{p_1}\right) \neq \left(\frac{a_i}{p_2}\right)\} = \{i \in \mathcal{I}' : \mathfrak{i}(\mathcal{P}) \text{ is odd}\}. \tag{10.3.2}$$

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

$$|\mathcal{L}| \leq \ell. \tag{10.3.3}$$

We see that $\left(\frac{a_i}{p_j}\right) = \left(\frac{n+id}{p_j}\right) = \left(\frac{i-i_j}{p_j}\right)\left(\frac{d}{p_j}\right)$ for $i \in \mathcal{I}'$ and $j = 1, 2$. Therefore $\mathcal{L} = \mathcal{I}_1$ or $\mathcal{I}_2$ according as $\left(\frac{d}{p_1}\right) \neq \left(\frac{d}{p_2}\right)$ or $\left(\frac{d}{p_1}\right) = \left(\frac{d}{p_2}\right)$, respectively. Now the assertion of the Lemma 10.3.2 follows from (10.3.2) and (10.3.3). □

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

Corollary 10.3.3. *Let $p_1, p_2, i_1, i_2, \mathcal{P}_0, \mathcal{P}, \mathcal{I}, \mathcal{I}', \mathcal{I}_1, \mathcal{I}_2$ and ℓ be as in Lemma 10.3.2. Assume that*

$$\ell < \frac{1}{2}|\mathcal{I}'|. \tag{10.3.4}$$

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

$$\mathcal{M} = \begin{cases} \mathcal{I}_1 & \text{if } |\mathcal{I}_1| < |\mathcal{I}_2| \\ \mathcal{I}_2 & \text{otherwise} \end{cases} \tag{10.3.5}$$

and

$$\mathcal{B} = \begin{cases} \mathcal{I}_2 & \text{if } |\mathcal{I}_1| < |\mathcal{I}_2| \\ \mathcal{I}_1 & \text{otherwise.} \end{cases} \tag{10.3.6}$$

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

Proof. We see from Lemma 10.3.2 that $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) \leq \ell$ and from (10.3.4) that $\max(|\mathcal{I}_1|, |\mathcal{I}_2|) \geq \frac{1}{2}|\mathcal{I}'| > \ell$. Now the assertion follows from Lemma 10.3.2. □

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

10.4. Lemmas for the Proof of Theorem 10.1.1 (contd.)

We recall that (2.1.1) is the equation (9.1.1) with $t = k$ and $\gamma_i = i - 1$ so that (9.1.2) and (9.1.3) give (2.1.2) and (9.1.4) is (2.1.3). Further we have $R = \{a_i : 0 \leq i < k\}$. For the proof of Theorem 10.1.1, we use the following Corollary which follows from Lemma 9.5.2.

Corollary 10.4.1. *For $a \in R$, let*

$$f_4(k, a, \delta) = \begin{cases} 1 & \text{if } k \leq a2^{3-\delta} \\ \bar{f}(\mathcal{K}_a) & \text{if } k > a2^{3-\delta}, 3|d \\ \bar{f}(\frac{\mathcal{K}_a}{3}) + \bar{f}(\frac{\mathcal{K}_a}{9}) & \text{if } k > a2^{3-\delta}, 3 \nmid d \end{cases}$$

and

$$g_4(k, a) = \begin{cases} 1 & \text{if } k \leq 4a \\ \lceil \frac{\mathcal{K}_a}{2} \rceil + 1 & \text{if } 4a < k \leq 32a \\ \bar{f}(\frac{\mathcal{K}_a}{2}) + \bar{f}(\frac{\mathcal{K}_a}{4}) & \text{if } k > 32a, 3|d \\ \bar{f}(\frac{\mathcal{K}_a}{6}) + \bar{f}(\frac{\mathcal{K}_a}{12}) + \bar{f}(\frac{\mathcal{K}_a}{18}) + \bar{f}(\frac{\mathcal{K}_a}{36}) & \text{if } k > 32a, 3 \nmid d. \end{cases}$$

Then we have

$$\nu_o(a) \leq f_4(k, a, \delta), \ \nu_e(a) \leq g_4(k, a)$$

and

$$\nu(a) \leq F_1(k, a, \delta) := \begin{cases} 1 & \text{if } k \leq a \\ f_4(k, a, \delta) & \text{if } k > a \text{ and } d \text{ even} \\ f_4(k, a, 0) + g_4(k, a) & \text{if } k > a \text{ and } d \text{ odd.} \end{cases}$$

Lemma 10.4.2. *Let k be a prime with $7 \le k \le 97$ and assume* (2.1.1)*. For $k \ge 11$, assume that Theorem 10.1.1 is valid for all primes k_1 with $7 \le k_1 < k$. For $11 \le k \le 29$, assume that $k \nmid d$ and $k \nmid n + id$ for $0 \le i < k - k'$ and $k' \le i < k$ where $k' < k$ are consecutive primes. Let $(q_1, q_2) = (5, 7)$ if $k = 7$; $(5, 11)$ if $k = 11$; $(11, 13)$ if $13 \le k \le 23$; $(19, 29)$ if $29 \le k \le 59$; $(59, 61)$ if $k = 61$; $(43, 67)$ if $k = 67, 71$; $(23, 73)$ if $k = 73, 79$; $(37, 83)$ if $k = 83$; $(79, 89)$ if $k = 89$ and $(23, 97)$ if $k = 97$. Then $q_1|d$ or $q_2|d$ unless $(a_0, a_1, \cdots, a_{k-1})$ is given by the following or their mirror images.*

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

We shall prove Lemma 10.4.2 in Section 10.5.

Lemma 10.4.3. *Let k be a prime with $29 \le k \le 97$ and Q_0 a prime dividing d. Assume* (2.1.1) *with $k \nmid d$ and $k \nmid n + id$ for $0 \le i < k - k'$ and $k' \le i < k$ where $k' < k$ are consecutive primes. Then there are primes Q_1 and Q_2 given in the following table such that either $Q_1|d$ or $Q_2|d$.*

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

The proofs of Lemmas 10.4.2 and 10.4.3 depend on the repeated application of Lemma 10.3.2 and Corollary 10.3.3. We shall prove Lemma 10.4.3 in section 10.6. Next we apply Lemmas 10.4.1, 9.5.3 and 10.4.3 to prove the following result.

Lemma 10.4.4. *Let k be a prime with $7 \le k \le 97$. Assume* (2.1.1) *with $k \nmid d$. Further for $k \ge 29$, assume that $k \nmid n + id$ for $0 \le i < k - k'$ and $k' \le i < k$ where $k' < k$ are consecutive primes. Let (q_1, q_2) be as in Lemma 10.4.2. Then $q_1 \nmid d$ and $q_2 \nmid d$.*

The Section 10.7 contains a proof of Lemma 10.4.4. Assume that $3 \nmid d$ and $5 \nmid d$. We define some more notation. For a subset $\mathcal{J} \subseteq [0, k) \cap \mathbb{Z}$, let

$$\mathcal{I}_3^0 = \mathcal{I}_3^0(\mathcal{J}) := \{i \in \mathcal{J} | i \equiv i_3 (\text{mod } 3)\},\ \mathcal{I}_3^+ = \mathcal{I}_3^+(\mathcal{J}) := \{i \in \mathcal{J} | \left(\frac{i - i_3}{3}\right) = 1\},$$
$$\mathcal{I}_3^- = \mathcal{I}_3^-(\mathcal{J}) := \{i \in \mathcal{J} | \left(\frac{i - i_3}{3}\right) = -1\}$$

and

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

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

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

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

$$(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (\{1\}, \{7\}, \{14\}, \{2\}) \text{ or } (\{7\}, \{1\}, \{2\}, \{14\}) \tag{10.4.1}$$

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

10.5. Proof of Lemma 10.4.2

Let $k' < k$ be consecutive primes. We may suppose that if (2.1.1) holds for some $k > 29$, then $k \nmid d$ and $k \nmid a_i$ for $0 \leq i < k - k'$ and $k' \leq i < k$, otherwise the assertion follows from Theorem 10.1.1 with k replaced by k'. The subsections 3.1 to 3.10 will be devoted to the proof of Lemma 10.4.2. We may assume that $q_1 \nmid d$ and $q_2 \nmid d$ otherwise the assertion follows.

10.5.1. The case $k = 7$. Then $5 \nmid d$. By taking mirror images (2.2.1) of (2.1.1), there is no loss of generality in assuming that $5|n + i_5 d, 7|n + i_7 d$ for some pair (i_5, i_7) with $0 \leq i_5 < 5, 0 \leq i_7 \leq 3$. Further we may suppose $i_7 \geq 1$, otherwise the assertion follows from the case $k = 6$. We apply Lemma 10.3.2 with $\mathcal{P}_0 = \emptyset, p_1 = 5, p_2 = 7$, $(i_1, i_2) = (i_5, i_7)$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \Lambda(5, 7) = \{2\}$ and $\ell \leq \ell_1 = \lceil \frac{k}{2} \rceil$ to conclude that either

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

or

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

Let $(i_5, i_7) = (3, 1)$. Then $\mathcal{I}_1 = \{0, 2, 6\}$ and $\mathcal{I}_2 = \{4, 5\}$. We see that $\mathcal{I}_1$ is covered by $\mathcal{P}$ and hence $\mathfrak{i}(\mathcal{P})$ is even for $i \in \mathcal{I}_2$. Thus $2 \nmid a_i$ for $i \in \mathcal{I}_2$. Therefore $a_4, a_5 \in \{1, 3\}$ and $a_0, a_2, a_6 \in \{2, 6\}$. If $a_0 = 6$ or $a_6 = 6$, then $3 \nmid a_4 a_5$ so that $a_4 = a_5 = 1$. This is not possible by modulo 3. Thus $a_0 = a_6 = 2$. Since $\left(\frac{a_0}{5}\right)\left(\frac{a_2}{5}\right) = \left(\frac{(-3d)(-d)}{5}\right) = -1$, we get $a_2 = 6$. Hence $a_4 = 1$. Further $a_5 = 3$ since $\left(\frac{a_5}{5}\right)\left(\frac{a_4}{5}\right) = \left(\frac{(2d)(1d)}{5}\right) = -1$. Also $5|a_3$ and $7|a_1$, otherwise the assertion follows from the results [**45**] for $k = 5$ and [**1**] for $k = 6$, respectively, stated in Section 7.2. In fact $a_1 = 7, a_3 = 5$ by $\gcd(a_1 a_3, 6) = 1$. Thus $(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (2, 7, 6, 5, 1, 3, 2)$. The proofs for the other cases of (i_5, i_7) are similar. We get $(a_0, \cdots, a_6) = (1, 5, 6, 7, 2, 1, 10)$ when $(i_5, i_7) = (1, 3)$, $(a_0, \cdots, a_6) = (1, 2, 7, 6, 5, 1, 3)$ when $(i_5, i_7) = (4, 2)$ and all the other pairs are excluded. Hence Lemma 10.4.2 with $k = 7$ follows. □

10.5.2. The case $k = 11$. Then $5 \nmid d$. By taking mirror images (2.2.1) of (2.1.1), there is no loss of generality in assuming that $5|n + i_5 d, 11|n + i_{11} d$ for some pair (i_5, i_{11}) with $0 \leq i_5 < 5, 4 \leq i_{11} \leq 5$. We apply Lemma 10.3.2 with $\mathcal{P}_0 = \emptyset, p_1 = 5, p_2 = 11$, $(i_1, i_2) = (i_5, i_{11})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \Lambda(5, 11) = \{3\}$ and $\ell \leq \ell_1 = \lceil \frac{k}{3} \rceil$ to derive that either

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

or

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

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

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

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

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

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

10.5.3. The cases $13 \le k \le 23$. Then $11 \nmid d$ and $13 \nmid d$. There is no loss of generality in assuming that $11|n + i_{11}d, 13|n + i_{13}d$ for some pair (i_{11}, i_{13}) with $0 \le i_{11} < 11, 0 \le i_{13} \le \frac{k-1}{2}$ and further $i_{13} \ge 2$ if $k = 13$. We have applied Lemma 10.3.2 once in each of cases $k = 7$ and $k = 11$ but we apply it twice for every case $13 \le k \le 23$ in this section. Let $\mathcal{P}_0 = \emptyset, p_1 = 11, p_2 = 13, (i_1, i_2) = (i_{11}, i_{13})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \mathcal{P}_1 := \Lambda(11, 13)$ and $\ell \le \ell_1$ where $\ell_1 = 3$ if $k = 13$; $\ell_1 = \lceil \frac{k}{5} \rceil + \lceil \frac{k}{17} \rceil$ if $k > 13$. Then $\ell_1 < \frac{1}{2}|\mathcal{I}'|$ since $|\mathcal{I}'| \ge k - \lceil \frac{k}{11} \rceil - \lceil \frac{k}{13} \rceil$. By Corollary 10.3.3, we derive that $\mathcal{I}'$ is partitioned into $\mathcal{M} =: \mathcal{M}_1$ and $\mathcal{B} =: \mathcal{B}_1$ such that $(\mathcal{M}_1, \mathcal{B}_1, \mathcal{P}_1, \ell_1)$ has *Property* $\mathfrak{H}$. Now we restrict to all such pairs (i_{11}, i_{13}) satisfying $|\mathcal{M}_1| \le \ell_1$ and $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. We check that $|\mathcal{M}_1| > 2$. Therefore $5 \nmid d$ since $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. Thus there exists i_5 with $0 \le i_5 < 5$ such that $5|n + i_5 d$.

Now we apply Lemma 10.3.2 with $p_1 = 5, p_2 = 11$ and partition $\mathcal{B}_1(5, 11)$ into two subsets. Let $\mathcal{P}_0 = \Lambda(11, 13) \cup \{11, 13\}$, $(i_1, i_2) = (i_5, i_{11}), \mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(5, 11) \subseteq \{3, 19, 23\}$ and $\ell \le \ell_2$ where $\ell_2 = 5, 6, 8, 11$ if $k = 13, 17, 19, 23$, respectively. Hence $\mathcal{B}_1'$ is partitioned into $\mathcal{I}_1$ and $\mathcal{I}_2$ satisfying either

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

or

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

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

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

$$\mathfrak{i}(\mathcal{P}_2) \text{ is even for } i \in B \text{ and } p \nmid a_i \text{ for } i \in B \text{ whenever } p \in \mathcal{P}_0, \tag{10.5.1}$$

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

By taking $\mathcal{J} = B$, we get $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^+ \cup \mathcal{I}_3^-$ and $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$. Then $p \in \{2, 7\}$ whenever $p|a_i$ with $i \in \mathcal{I}_3^+ \cup \mathcal{I}_3^-$ by (10.5.1). By computing $\mathcal{I}_3^+, \mathcal{I}_3^-$, we find that i's have the same parity in exactly one of $\mathcal{I}_3^+, \mathcal{I}_3^-$. Therefore we get from (10.4.1) that

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

Let $k = 13$ and $(i_{11}, i_{13}) = (4, 2)$. Then we have $\mathcal{M}_1 = \{0, 5, 10\}$, $i_5 = 0, M = \{3, 9, 12\}$ and $B = \{1, 6, 7, 8, 11\}$ since the latter set is not covered by $\mathcal{P}_2 = \{3\}$. Further $i_3 = 0$, $\mathcal{I}_3^0 = \{6\}$, $\mathcal{I}_3^1 = \mathcal{I}_3^- = \{8, 11\}$, $\mathcal{I}_3^2 = \mathcal{I}_3^+ = \{1, 7\}$, $\mathcal{I}_5^+ = \{1, 6, 11\}, \mathcal{I}_5^- = \{7, 8\}$, $\mathcal{J}_1 = \{11\}, \mathcal{J}_2 = \{8\}$, $\mathcal{J}_3 = \{1\}, \mathcal{J}_4 = \{7\}$. Therefore $a_{11} = 1, a_8 = 7, a_1 = 14, a_7 = 2$ or $a_{11} = 7, a_8 = 1, a_1 = 2, a_7 = 14$. The second possibility is excluded since $a_{11} = 7, a_7 = 14$ is not possible. Further from (10.5.1), we get $a_6 = 1$ since $2 \nmid a_6$ and $7 \nmid a_6$. Since $13|n + 2d$ and $7|n + d$, we get $\left(\frac{i-2}{13}\right) = \left(\frac{a_i a_6}{13}\right) = \left(\frac{a_i}{13}\right)$ and $-\left(\frac{i-1}{7}\right) = \left(\frac{a_i a_6}{7}\right) = \left(\frac{a_i}{7}\right)$. We observe that $13|n{+}2d, 11|n{+}4d, 7|n{+}d, 5|n, 3|n, 2|n{+}d, 5|a_i$ for $i \in \mathcal{M}$ and $3|a_i$ for $i \in \mathcal{M}_1$. Now we see that $a_0 \in \{5, 15\}$ and $a_0 = 5$ is excluded since $\left(\frac{5}{7}\right) \ne -\left(\frac{-1}{7}\right)$. Thus $a_0 = 15$. Next $a_1 = 14, a_2 = 13$ and $a_3 = 3$. Also $a_4 \in \{1, 11\}$ and $a_4 \ne 1$ since $\left(\frac{a_4}{13}\right) = \left(\frac{2}{13}\right) = -1$. Similarly we derive that $a_5 = 10, a_6 = 1, a_7 = 2, a_8 = 7, a_9 = 6, a_{10} = 5, a_{11} = 1$ and $a_{12} = 3$. Thus $(a_0, a_1, \cdots, a_{12}) = (15, 14, 13, \cdots, 5, 1, 3)$. The other case $(i_{11}, i_{13}) = (5, 3)$ is similar and we get $(a_0, a_1, \cdots, a_{12}) = (1, 15, 14, \cdots, 5, 1)$.

Let $k = 17$ and $(i_{11}, i_{13}) = (0, 0)$. Then we have $\mathcal{M}_1 = \{5, 10, 15\}$ and $i_5 = 0$. We see from the assumption of Lemma 10.4.2 with $k = 17, k' = 13$ that $4 \le i_{17} < 13$. Hence, from $i_{17} \in \bigcup\limits_{p=5,11,13} \{i_p + pj : 0 \le j < \lceil \frac{k}{p} \rceil\}$, we get $i_{17} \in \{5, 10, 11\}$. Further $M = \{3, 6, 12\}, B = \{1, 2, 4, 7, 8, 9, 14, 16\}$, $i_3 = 0$, $\mathcal{I}_3^0 = \{9\}$, $\mathcal{I}_3^1 = \{1, 4, 7, 16\}$, $\mathcal{I}_3^2 = \{2, 8, 14\}$, $\mathcal{I}_5^+ = \{1, 4, 9, 14, 16\}, \mathcal{I}_5^- = \{2, 7, 8\}$, $\mathcal{J}_1 = \{1, 4, 16\}$, $\mathcal{J}_2 = \{7\}$, $\mathcal{J}_3 = \{14\}$ and $\mathcal{J}_4 = \{2, 8\}$. Therefore $a_1 = a_4 = a_{16} = 1, a_7 = 7, a_{14} = 14, a_2 = a_8 = 2$. Thus $a_9 = 1$ by (10.5.1) and $2 \nmid a_9, 7 \nmid a_9$. Now we see by Legendre symbol mod 17 that $a_1 = a_4 = a_9 = a_{16} = 1$ is not possible. The case $(i_{11}, i_{13}) = (5, 3)$ is excluded similarly.

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

Let $k = 23$ and $(i_{11}, i_{13}) = (0, 0)$. Then $\mathcal{M}_1 = \{5, 10, 15, 17, 20\}$, $i_5 = 0, i_{17} = 0$, $M = \{3, 6, 12, 19, 21\}$, $B = \{1, 2, 4, 7, 8, 9, 14, 16, 18\}$, $i_3 = 0$ and $i_{19} = 0$ since $23 \nmid a_{19}$. We have $i_{23} \in \{5, 6, 9, 10, 11, 12, 13, 15, 17, 18\}$ since $4 \le i_{23} < 19$. Here we observe that $23 \nmid a_{19}$ and $4 \le i_{23} < 19$ in view of our assumption that $k \nmid a_i$ for $0 \le i < k - k'$ and $k' \le i < k$ with $k = 23, k' = 19$. Further $\mathcal{I}_3^0 = \{9, 18\}$, $\mathcal{I}_3^1 = \{1, 4, 7, 16\}$, $\mathcal{I}_3^2 = \{2, 8, 14\}$, $\mathcal{I}_5^+ = \{1, 4, 9, 14, 16\}, \mathcal{I}_5^- = \{2, 7, 8, 18\}$, $\mathcal{J}_1 = \{1, 4, 16\}, \mathcal{J}_2 = \{7\}$, $\mathcal{J}_3 = \{14\}$ and $\mathcal{J}_4 = \{2, 8\}$. Therefore $a_1 = a_4 = a_{16} = 1, a_7 = 7, a_{14} = 14, a_2 = a_8 = 2$. This is not possible since $\left(\frac{a_1}{23}\right) = \left(\frac{a_4}{23}\right) = \left(\frac{a_{16}}{23}\right) = \left(\frac{a_2}{23}\right) = \left(\frac{a_8}{23}\right) = 1$. The cases $(i_{11}, i_{13}) = (0, 9), (1, 10), (2, 11), (4, 0), (7, 9), (8, 10), (9, 11)$ are excluded similarly. Let $(i_{11}, i_{13}) = (5, 1)$. Then $\mathcal{M}_1 = \{7, 10, 12, 17, 22\}$, $i_5 = 2, i_{17} = 10$, $M = \{0, 3, 4, 6, 8, 15, 21\}$, $B = \{9, 11, 13, 18, 19, 20\}$ and $i_3 = 0$. This implies either $23|a_4, 19|a_8$ or $23|a_8, 19|a_4$. Further $\mathcal{I}_3^0 = \{9, 18\}$, $\mathcal{I}_3^1 = \{11, 20\}$, $\mathcal{I}_3^2 = \{13, 19\}$, $\mathcal{I}_5^+ = \{11, 13, 18\}$, $\mathcal{I}_5^- = \{9, 19, 20\}$, $\mathcal{J}_1 = \{11\}, \mathcal{J}_2 = \{20\}$, $\mathcal{J}_3 = \{13\}$ and $\mathcal{J}_4 = \{19\}$. Therefore $a_{11} = 1, a_{20} = 7, a_{13} = 14, a_{19} = 2$. Further from (10.5.1), we get $a_9 \in \{1, 2\}, a_{18} = 1$ since $7 \nmid a_9 a_{18}, 2 \nmid a_{18}$. However $a_9 = 2$ as $9 \in \mathcal{I}_5^-, 18 \in \mathcal{I}_5^+$. Since $\left(\frac{a_{11}}{23}\right) = \left(\frac{a_{18}}{23}\right) = 1$, we see that $23|a_4, 19|a_8$. By using $\left(\frac{a_i}{p}\right) = \left(\frac{a_i a_{11}}{p}\right) = \left(\frac{(i-i_p)(11-i_p)}{p}\right)$, we get $\left(\frac{a_i}{23}\right) = -\left(\frac{i-4}{23}\right)$, $\left(\frac{a_i}{11}\right) = -\left(\frac{i-5}{11}\right)$, $\left(\frac{a_i}{7}\right) = -\left(\frac{i-6}{7}\right)$ and $\left(\frac{a_i}{5}\right) = \left(\frac{i-2}{5}\right)$. Now from $23|a_4, 19|a_8, 17|a_{10}, 13|n + d, 11|n + 5d, 7|n + 6d, 5|n + 2d, 3|n, 2|n + d$, $\mathcal{M}_1$ is covered by $\{5, 17\}$, M is covered by $\{3, 19, 23\}$, we derive that $(a_0, a_1, \cdots, a_{22}) = (3, 26, \cdots, 6, 5)$. The pairs $(i_{11}, i_{13}) = (5, 7), (6, 2), (6, 8)$ are similar and we get $(a_0, a_1, \cdots, a_{22}) = (6, 7, \cdots, 3, 7)$,
$(7, 3, \cdots, 7, 6), (5, 6, 7, \cdots, 3)$, respectively. □

10.5.4. Introductory remarks on the cases $k \ge 29$. Assume $q_1 \nmid d$ and $q_2 \nmid d$. Then, by taking mirror image (2.2.1) of (2.1.1), there is no loss of generality in assuming that $q_1|n+i_{q_1}d, q_2|n+i_{q_2}d$ for some pair (i_{q_1}, i_{q_2}) with $0 \le i_{q_1} < q_1, 0 \le i_{q_2} \le \frac{k-1}{2}$ and further $i_{q_2} \ge k - k'$ if $q_2 = k$. For $k = 61$, by taking $(n + 8d) \cdots (n + 60d)$ and $k = 53$, we may assume that $\max(i_{59}, i_{61}) \ge 8$ if $i_{59} \ge 2$. Let $\mathcal{P}_0 = \emptyset, p_1 = q_1, p_2 = q_2, (i_1, i_2) = (i_{q_1}, i_{q_2})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$, $\mathcal{P} = \mathcal{P}_1 := \Lambda(q_1, q_2)$ and $\ell \le \ell_1 = \sum_{p \in \mathcal{P}_1} \lceil \frac{k}{p} \rceil$. We check that $\ell_1 < \frac{1}{2}|\mathcal{I}'|$ since $|\mathcal{I}'| \ge k - \lceil \frac{k}{q_1} \rceil - \lceil \frac{k}{q_2} \rceil$. By Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_1$ and $\mathcal{B} =: \mathcal{B}_1$ with $(\mathcal{M}_1, \mathcal{B}_1, \mathcal{P}_1, \ell_1)$ having *Property* $\mathfrak{H}$. We now restrict to all such pairs (i_{q_1}, i_{q_2}) for which $|\mathcal{M}_1| \le \ell_1$ and $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. We find that there is no such pair (i_{q_1}, i_{q_2}) when $k = 97$.

10.5.5. The cases $29 \le k \le 59$. As stated in Lemma 10.4.2, we have $q_1 = 19, q_2 = 29$ and $\mathcal{P}_1 = \Lambda(19, 29) \subseteq \{11, 13, 17, 43, 47, 53, 59\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by

$$\begin{aligned}
k = 29 &: (0,9),(1,10),(2,11),(3,12),(4,13),(15,5),(16,6),(17,7),(18,8);\\
k = 31 &: (0,0),(0,9),(1,10),(2,11),(3,12),(4,13),(11,1),\\
&\quad (12,2),(13,3),(14,4),(15,5),(16,6),(17,7),(18,8);\\
k = 37 &: (0,0),(0,9),(1,10),(2,11),(3,12),(4,13),(17,7),(18,8);
\end{aligned}$$

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

Let $k = 31$ and $(i_{19}, i_{29}) = (0, 9)$. We see that $\mathcal{P}_1 = \{11, 13, 17\}$, $\mathcal{M}_1 = \{4, 5, 12, 16, 21, 25, 27\}$ and $\mathcal{B}_1 = \{1, 2, 3, 6, 7, 8, 10, 11, 13, 14, 15, 17, 18, 20, 22, 23, 24, 26, 28, 29, 30\}$. Since $\mathcal{M}_1$ is covered by $\mathcal{P}_1$, we get 11 divides a_5, a_{16}, a_{27}; 13 divides a_{12}, a_{25} and 17 divides a_4, a_{21} so that $i_{11} = 5, i_{13} = 12, i_{17} = 4$. We see that $\gcd(11 \cdot 13 \cdot 17, a_i) = 1$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{19, 29\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (i_{11}, i_{13}) = (5, 12), \mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31\}$ and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil \frac{k}{p} \rceil = 8$. Thus $|\mathcal{I}'| = |\mathcal{B}_1| = 21 > 2\ell_2$. Then the condition of Corollary 10.3.3 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$. We get $\mathcal{M}_2 = \{1, 3, 7, 8, 18, 23, 28\}$. This is not possible since $\mathcal{M}_2$ is not covered by $\mathcal{P}_2$. Further the following pairs (i_{19}, i_{29}) are excluded similarly:

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

Thus $k > 29$.

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

$$i_{59} \in \mathcal{M}_1 \cup \{19, 29, 38\} \cup \{6, 10\}. \tag{10.5.2}$$

Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{19, 29\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (0, 0), \mathcal{I} = \mathcal{B}_1 \setminus \{4, 6, 10\}$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31, 37\}$ and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \lceil \frac{k}{p} \rceil = 16$. Thus $|\mathcal{I}'| = |\mathcal{B}_1| - 2 > 2\ell_2$. Then the conditions of Corollary 10.3.3 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ with $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ having *Property* $\mathfrak{H}$. We get $\mathcal{M}_2 = \{5, 15, 20, 30, 31, 35, 37, 40, 45\}$, $\mathcal{B}_2 = \{1, 2, 3, 7, 8, 9, 12, 14, 16, 18, 21, 23, 24, 25, 27, 28, 32, 36, 41, 42, 46, 48, 49, 50, 54, 56\}$, $i_5 = 0$, $31|a_{31}, 37|a_{37}$ or $31|a_{37}, 37|a_{31}$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{19, 29\}, p_1 = 5, p_2 = 11$, $(i_1, i_2) := (0, 0), \mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 23, 41\}$ and $\ell \le \ell_3 = \sum_{p \in \mathcal{P}_3} \lceil \frac{k}{p} \rceil$. Then by Lemma 10.3.2, we see that $M = \{3, 6, 12, 21, 23, 24, 27, 41, 42, 46, 48, 54\}$ is covered by $\mathcal{P}_3$ and $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B = \{1, 2, 7, 8, 9, 14, 16, 18, 28, 32, 36, 49, 56\}$. Thus $i_3 = i_{23} = i_{41} = 0$ and $p \in \{2, 7\}$ whenever

$p|a_i$ with $i \in B$. Putting $\mathcal{J} = B$, we have $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^2$ and $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

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

and

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

so that

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

Hence $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4) \subseteq (\{1\}, \{7\}, \{14\}, \{2\})$ by (10.4.1). Thus $a_1 = a_{16} = a_{49} = 1$, $a_7 = a_{28} = 7, a_{14} = a_{56} = 14, a_2 = a_8 = a_{32} = 2$. Further we get $a_9 = a_{36} = 1$ and $a_{18} = 2$ since $9, 36 \in \mathcal{I}_5^+$ and $18 \in \mathcal{I}_5^-$. Since

$$\left(\frac{a_i}{59}\right) = 1 \text{ for } a_i \in \{1, 7\}, \tag{10.5.3}$$

we see that $\left(\frac{a_i}{59}\right) = 1$ for $i \in \{1, 7, 9, 16, 28, 36, 49\}$ which is not possible by (10.5.2).

Let $k = 41$ and $(i_{19}, i_{29}) = (2, 11)$. Then we see that $\mathcal{P}_1 = \{11, 13, 17\}$, $\mathcal{M}_1 = \{1, 6, 7, 14, 18, 23, 27, 29\}$, $\mathcal{B}_1 = \{0, 3, 4, 5, 8, 9, 10, 12, 13, 15, 16, 17, 19, 20, 22, 24, 25, 26, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39\}$, $i_{11} = 7$, $i_{13} = 1, i_{17} = 6$. Further $\gcd(a_i, 11 \cdot 13 \cdot 17) = 1$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{19, 29\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (7, 1), \mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31, 37\}$ and $\ell \leq \ell_2 = \sum_{p \in \mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 13$. Then $|\mathcal{I}'| = |\mathcal{B}_1| > 2\ell_2$. Thus the conditions of Corollary 10.3.3 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$ and $\mathcal{B} =: \mathcal{B}_2$ such that $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$. We have $\mathcal{M}_2 = \{0, 3, 5, 9, 10, 20, 25, 30, 35\}$, $\mathcal{B}_2 = \{4, 8, 12, 13, 15, 16, 17, 19, 22, 24, 26, 28, 31, 32, 33, 34, 36, 37, 38, 39\}$, $i_5 = 0$. Further $31 \cdot 37 | a_3 a_9$, $31 \nmid a_{34}$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{19, 29\}, p_1 = 5, p_2 = 11$, $(i_1, i_2) := (0, 7), \mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 23, 41\}$, $\ell \leq \sum_{p \in \mathcal{P}_3} \left\lceil \frac{k}{p} \right\rceil$ and apply Lemma 10.3.2 to see that $M = \{13, 16, 17, 19, 28, 34, 37\}$ is covered by $\mathcal{P}_3$, $i_3 = 1$, $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B = \{4, 8, 12, 22, 24, 26, 31, 32, 33, 36, 38, 39\}$. Further $i_{23} = 17$, $i_{41} \in \{2, 11, 21\} \cup \mathcal{M}_1 \cup \mathcal{M}_2 \cup M \cup \{4, 22, 31\}$ or vice-versa. Here we observe that i_{41} exists since $41 \nmid d$. Thus $23 \cdot 41 | \prod a_i$ where i runs through the set $\{2, 11, 21\} \cup \mathcal{M}_1 \cup \mathcal{M}_2 \cup \{4, 22, 31\}$. Therefore $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{I}_3^1 \cup \mathcal{I}_3^2$ where $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^2$, $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

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

and

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

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

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

and $a_{24} = a_{36} = a_{39} = 1, a_{12} = a_{33} = 7, a_{26} = 14, a_8 = a_{32} = a_{38} = 2$ by (10.4.1). Since

$$\left(\frac{a_i}{41}\right) = 1 \text{ for } a_i \in \{1, 2\}, \tag{10.5.4}$$

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

All other cases are excluded similarly. Analogous to (10.5.3) and (10.5.4), we use $\left(\frac{a_i}{k}\right) = 1$ for

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

to exclude the remaining possibilities. □

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

Let $(i_{59}, i_{61}) = (8, 6)$. Then $\mathcal{P}_1 = \{7, 13, 17, 29, 47, 53\}$, $\mathcal{M}_1 = \{2, 4, 9, 11, 14, 15, 16, 20, 25, 28, 32, 33, 38, 39, 41, 46, 50, 53, 54, 60\}$, $\mathcal{B}_1 = \{0, 1, 3, 5, 7, 10, 12, 13, 17, 18, 19, 21, 22, 23, 24, 26, 27, 29, 30, 31, 34, 35, 36, 37, 40, 42, 43, 44, 45, 47, 48, 49, 51, 52, 55, 56, 57, 58, 59\}$, $i_7 = 4, i_{13} = 2, i_{17} = 16, i_{29} = 9$ and a_{14}, a_{20} are divisible by $47, 53$. Further $\gcd(p, a_i) = 1$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. Let $\mathcal{P}_0 = \mathcal{P}_1 \cup \{59, 61\}, p_1 = 7, p_2 = 17, (i_1, i_2) := (4, 16), \mathcal{I} = \mathcal{B}_1, \mathcal{P} = \mathcal{P}_2 := \Lambda(7, 17) \backslash \mathcal{P}_0 = \{11, 19, 23, 37\}$ and $\ell \leq \ell_2 = \sum_{p \in \mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 15$. Then $2\ell_2 < |\mathcal{I}'| = |\mathcal{B}_1| - 1$. By Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$

and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$. We find that $\mathcal{M}_2 = \{1, 10, 12, 21, 23, 29, 30, 34, 44, 45, 48, 56\}$, $\mathcal{B}_2 = \{0, 3, 5, 7, 13, 17, 19, 22, 24, 26, 27, 31, 35, 36, 37, 40, 42, 43, 47, 49, 51, 52, 55, 57, 58, 59\}$, $i_{11} = 1, i_{19} = 10$, $i_{23} = 21, i_{37} = 30$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{59, 61\}$, $p_1 = 11, p_2 = 59$, $(i_1, i_2) := (1, 8)$, $\mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 59) \setminus \mathcal{P}_0 = \{31, 41\}$ and $\ell \le \ell_3 = \sum_{p \in \mathcal{P}_3} \left\lceil \frac{k}{p} \right\rceil = 4$. Then $2\ell_3 < |\mathcal{I}'| = |\mathcal{B}_2|$. By Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_3$ and $\mathcal{B} =: \mathcal{B}_3$ such that $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ has *Property* $\mathfrak{H}$. We get $\mathcal{M}_3 = \{0, 5, 26, 36\}$ which cannot be covered by $\mathcal{P}_3$. This is a contradiction. The remaining cases are excluded similarly. □

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

$$k = 67 : (i, i), 6 \le i \le 33;$$
$$k = 71 : (i, i), 0 \le i \le 35, i \ne 24, 25 \text{ and } (24, 0), (25, 1), (26, 2), (27, 3).$$

Let $k = 71$ and $(i_{43}, i_{67}) = (27, 3)$. We see that $\mathcal{P}_1 = \{11, 13, 19, 29, 31, 37, 41, 53, 71\}$, $\mathcal{M}_1 = \{4, 5, 8, 12, 13, 15, 17, 18, 26, 29, 31, 32, 33, 37, 39, 41, 44, 48, 51, 57, 59\}$, $\mathcal{B}_1 = \{0, 1, 2, 6, 7, 9, 10, 11, 14, 16, 19, 20, 21, 22, 23, 24, 25, 28, 30, 34, 35, 36, 38, 40, 42, 43, 45, 46, 47, 49, 50, 52, 53, 54, 55, 56, 58, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69\}$, $i_{11} = 4, i_{13} = 5, i_{19} = 13$. Therefore $\{8, 12, 17, 29, 33, 39, 41\}$ is covered by $29, 31, 37, 41, 53, 71$ implying either $i_{29} = 12$ or $i_{29} \in \{17, 29, 33\}$, $i_{31} = 8$. Let $i \in \mathcal{B}_1$ and $p | a_i$ with $p \in \mathcal{P}_1$. Then there is a $q \in \mathcal{P}_1$ such that $pq | a_i$ since $\mathfrak{i}(\mathcal{P}_1)$ is even. Next we consider the case $i_{31} = 8$. Then $\{12, 17, 29, 33, 41\} =: \mathcal{M}_1'$ is covered by $29, 37, 41, 53, 71$ and $i_{29} \ne 12$. For $29 \in \mathcal{M}_1'$, we may suppose that either $29 | a_{29}, 41 | a_{17}, 29 \cdot 41 | a_{58}$ or $29 | a_{29}, 41 | a_{41}, 29 \cdot 41 | a_0$. Thus 0 or 58 in $\mathcal{B}_1$ correspond to 29. We argue as above that for any other element of $\mathcal{M}_1'$, there is no corresponding element in $\mathcal{B}_1$. For the first case, we derive similarly that $31 | a_{33}, 37 | a_{39}, 31 \cdot 37 | a_2$ or $37 | a_{17}, 37 \cdot 71 | a_{54}$ or $37 | a_{29}, 37 \cdot 71 | a_{63}$ or $41 | a_{17}, 37 \cdot 71 | a_{58}$. Therefore

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

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

$$i_{71} \in \mathcal{M}_1 \cup \{27\} \cup \mathcal{B}_1' \text{ and } i_{71} \ne 32. \tag{10.5.5}$$

For each possibility $i_{29} \in \{0, 4, 12, 17\}$, we now take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{43, 67\}$, $p_1 = 19, p_2 = 29$, $(i_1, i_2) := (13, i_{29}), \mathcal{I} = \mathcal{B}_1 \setminus \mathcal{B}_1'$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(19, 29) \setminus \mathcal{P}_0 = \{17, 47, 59, 61\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 11$. Then $|\mathcal{I}'| = |\mathcal{B}_1| - 4 > 2\ell_2$. Thus the conditions of Corollary 10.3.3 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$ and $\mathcal{B} =: \mathcal{B}_2$ with $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ having *Property* $\mathfrak{H}$. We check that $|\mathcal{M}_2| \le \ell_2$ only at $i_{29} = 12$ in which case we get $\mathcal{M}_2 = \{9, 11, 19, 23, 36, 53\}$, $\mathcal{B}_2 = \{0, 1, 6, 7, 10, 14, 6, 20, 21, 22, 24, 25, 28, 30, 34, 35, 38, 40, 42, 43, 45, 46, 47, 49, 50, 52, 55, 56, 60, 61, 62, 63, 64, 65, 67, 68, 69\}$, $i_{17} = 2$, $\{9, 11, 23\}$ is covered by $47, 59, 61$. Thus $47 \cdot 59 \cdot 61 \mid a_9 a_{11} a_{23}$. Further $p \nmid a_i$ for $i \in \mathcal{B}_2$ and $p \in \mathcal{P}_2$. We now take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{43, 67\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (4, 5), \mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5\}$ and $\ell = \ell_3 = \left\lceil \frac{k}{5} \right\rceil = 15$. Then $|\mathcal{I}'| = |\mathcal{B}_2| > 2\ell_3$. By Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_3$ and $\mathcal{B} =: \mathcal{B}_3$ such that $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ has *Property* $\mathfrak{H}$. We calculate $\mathcal{M}_3 = \{0, 10, 25, 30, 35, 40, 50, 55, 60, 65\}$, $\mathcal{B}_3 = \{1, 6, 7, 14, 16, 20, 21, 22, 24, 28, 34, 38, 42, 43, 45, 46, 47, 49, 52, 54, 56, 58, 61, 62, 63, 64, 66, 67, 68, 69\}$, $i_5 = 0$ and further $5 \nmid a_{20} a_{45}$. Lastly we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{43, 67\}$, $p_1 = 5, p_2 = 11$, $(i_1, i_2) := (0, 4), \mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 23\}$ and $\ell = \ell_4 = \sum_{p \in \mathcal{P}_4} \left\lceil \frac{k}{p} \right\rceil$. By Lemma 10.3.2, we see that $M = \{16, 22, 24, 28, 43, 46, 47, 49, 64, 67\}$ is covered by $\mathcal{P}_4$, $i_3 = i_{23} = 1$, $B = \{1, 6, 7, 14, 21, 34, 38, 42, 52, 56, 61, 62, 63, 68, 69\}$ and hence $3 \nmid a_7 a_{34} a_{52} a_{61}$ and possibly $3 \cdot 23 | a_1$. Therefore $a_i \in \{1, 2, 7, 14\}$ for $i \in B \setminus \{1\}$. By taking $\mathcal{J} = B \setminus \{1\}$, we have $B \setminus \{1\} = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^- = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

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

and

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

Therefore

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

and hence $a_6 = a_{21} = a_{69} = 1, a_{42} = a_{63} = 7, a_{14} = a_{56} = 14, a_{38} = a_{62} = a_{68} = 2$ by (10.4.1). Further we get $a_{34} = a_{61} = 1$ and $a_{52} = 2$ by taking residue classes modulo 5. Since $\left(\frac{1}{71}\right) = \left(\frac{2}{71}\right) = 1$, we see that $\left(\frac{a_i}{71}\right) = 1$ for $i \in \{6, 21, 34, 38, 52, 61, 62, 68, 69\}$ which is not valid by the possibilities of i_{71} given by (10.5.5).

Let $k = 67$ and $(i_{43}, i_{67}) = (9, 9)$. We see that $\mathcal{P}_1 = \{11, 13, 19, 29, 31, 37, 41, 53\}$, $\mathcal{M}_1 = \{20, 22, 28, 31, 35, 38, 40, 42, 46, 47, 48, 50, 53, 61, 62, 64, 66\}$, $\mathcal{B}_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 23, 24, 25, 26, 27, 29, 30, 32, 33, 34, 36, 37, 39, 41, 43, 44, 45, 49, 51, 54, 55, 56, 57, 58, 59, 60, 63, 65\}$, $i_{11} = i_{13} = i_{19} = 9$ and $\{38, 40, 46, 50, 62\}$ is covered by $29, 31, 37, 41, 53$. Further $p \nmid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$ except possibly when $29|a_{50}, 41|a_{62}, 29 \cdot 41|a_{21}$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{43, 67\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (9, 9), \mathcal{I} = \mathcal{B}_1 \setminus \{21\}$ and $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 17, 47, 59, 61\}$. If $5 \nmid d$, we observe that there is at least 1 multiple of 5 among $n + (i_{11} + 11i)d$, $0 \le i \le 5$ and $\ell \le \sum_{p\in\mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil - 1 = 23$. Thus we always have $\ell \le 23 = \ell_2$. Then $|\mathcal{I}'| = |\mathcal{B}_1| - 1 > 2\ell_2$ since $|\mathcal{B}_1| = 48$. Thus the conditions of Corollary 10.3.3 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$. We have $\mathcal{M}_2 = \{0, 1, 2, 3, 5, 6, 7, 8, 14, 19, 24, 26, 29, 39, 43, 44, 49, 54, 56, 60\}$ which cannot be covered by $\mathcal{P}_2$. This is a contradiction. The cases $k = 67, (i_{43}, i_{67}) = (i, i)$ with $9 \le i \le 28$ and $k = 71, (i_{43}, i_{67}) = (i, i)$ with $13 \le i \le 28, i \ne 24, 25$ are excluded similarly as in this paragraph. The remaining cases are excluded similarly as $k = 71, (i_{43}, i_{67}) = (27, 3)$ given in the preceding paragraph. □

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

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

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

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

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

Further we have

$$i_{79} \in \{10, 15, 16, 18, 19, 30, 40, 46, 48\} \tag{10.5.6}$$

and either $i_{29} = 19$ or $i_{29} \in \{1, 10, 16, 18\}$, $i_{31} = 15$, $i_{37} = 3, i_{59} = 19$. Also for $p \in \mathcal{P}_1$, we have $p \nmid a_i$ for $i \in \mathcal{B}_1$ since $\mathfrak{i}(\mathcal{P}_1)$ is even for $i \in \mathcal{B}_1$. For each possibility $i_{29} \in \{1, 10, 16, 18, 19\}$, we now take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{23, 73\}$, $p_1 = 19, p_2 = 29$, $(i_1, i_2) := (1, i_{29}), \mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(19, 29) \setminus \mathcal{P}_0 = \{11, 17, 43, 53, 71\}$ and $\ell = \ell_2 = \sum_{p\in\mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 19$. Then $|\mathcal{I}'| \ge |\mathcal{B}_1| - 2 > 2\ell_2$. Thus the conditions of Corollary 10.3.3 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$ implying $i_{29} = 19$ in which case we get $\mathcal{M}_2 = \{0, 6, 9, 11, 22, 24, 26, 33, 34, 43, 44, 55, 60, 66\}$, $\mathcal{B}_2 = \{2, 5, 7, 13, 14, 17, 21, 23, 27, 28, 29, 32, 35, 36, 37, 41, 42, 45, 47, 49, 50, 52, 53, 56, 57, 59, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76\}$, $i_{11} = 0, i_{17} = 9$, $\{6, 24, 34\}$ is covered by $43, 53, 71$. Thus $43 \cdot 53 \cdot 71 \mid a_6 a_{24} a_{34}$. Further $p \nmid a_i$ for $i \in \mathcal{B}_2$ and $p \in \mathcal{P}_2$. We now take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{23, 73\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (0, 12), \mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5\}$ and $\ell = \ell_3 = \left\lceil \frac{k}{5} \right\rceil = 16$. Then $|\mathcal{I}'| = |\mathcal{B}_2| > 2\ell_3$. By Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_3$ and $\mathcal{B} =: \mathcal{B}_3$ with $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ having *Property* $\mathfrak{H}$. We calculate $\mathcal{M}_3 = \{7, 17, 32, 37, 42, 47, 57, 62, 67, 72\}$, $\mathcal{B}_3 = \{2, 5, 13, 14, 21, 23, 27, 28, 29, 35, 36, 41, 45, 49, 50, 52, 53, 56, 59, 61, 63, 65, 68, 69, 70, 71, 73, 74, 75, 76\}$, $i_5 = 2$ and $5 \nmid a_i$ for $i \in \mathcal{B}_3$. Lastly we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{23, 73\}$, $p_1 = 5, p_2 = 11$, $(i_1, i_2) := (2, 0), \mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41\}$ and $\ell = \ell_4 = \sum_{p\in\mathcal{P}_4} \left\lceil \frac{k}{p} \right\rceil$. By Lemma 10.3.2, we see that $M = \{23, 29, 35, 36, 50, 53, 56, 65, 71, 74\}$ is covered by $\mathcal{P}_4$, $i_3 = 2, i_{41} = 36$,

$B = \{5, 13, 14, 21, 28, 41, 45, 49, 59, 61, 63,$
$68, 69, 70, 73, 75, 76\}$ and hence $a_i \in \{1, 2, 7, 14\}$ for $i \in B$. By taking $\mathcal{J} = B$, we have $B = \mathcal{I}_3^0 \cup \mathcal{I}_3^1 \cup \mathcal{I}_3^- = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

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

and

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

Thus

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

and hence $a_{13} = a_{28} = a_{61} = a_{76} = 1, a_{49} = a_{70} = 7, a_{21} = a_{63} = 14, a_{45} = a_{69} = a_{75} = 2$ by (10.4.1). Further we get $a_{41} = a_{68} = 1$ and $a_5 = a_{59} = 2$ by residue modulo 5. Since $\left(\frac{1}{79}\right) = \left(\frac{2}{79}\right) = 1$, we see that $\left(\frac{a_i}{71}\right) = 1$ for $i \in \{5, 13, 28, 41, 45, 59, 61, 68, 69, 75, 76\}$ which is not valid by the possibilities of i_{79} given by (10.5.6). The other cases are excluded similarly. □

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

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

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

Let $(i_{37}, i_{83}) = (13, 4)$. We see that $\mathcal{P}_1 = \{17, 23, 29, 31, 47, 53, 59, 61, 67, 71, 73\}$, $\mathcal{M}_1 = \{0, 2, 14, 16, 18, 19, 20, 25, 26, 28, 29, 34, 36, 40, 41, 53, 56, 58, 64, 70\}$, $\mathcal{B}_1 = \{1, 3, 5, 6, 7, 8, 9, 10, 11, 12, 15, 17, 21, 22, 23, 24, 27, 30, 31, 32, 33, 35, 37, 38, 39, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 54, 55, 57, 59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82\}$, $i_{17} = 2, i_{23} = 18, i_{29} = 0$, $i_{31} = 25$ and $\{14, 16, 20, 26, 28, 34, 40\}$ is covered by $47, 53, 59, 61, 67, 71, 73$. Further $p \nmid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. For each possibility $i_{73} \in \{14, 16, 20, 26, 28, 34, 40\}$, we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{37, 83\}$, $p_1 = 23, p_2 = 73$, $(i_1, i_2) := (18, i_{73})$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(23, 73) \setminus \mathcal{P}_0 = \{13, 19, 79\}$ and $\ell = \ell_2 = \sum_{p \in \mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 14$. Then $|\mathcal{I}'| = |\mathcal{B}_1| > 2\ell_2$. Thus the conditions of Corollary 10.3.3 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$ which is possible only if $i_{73} = 14$. Then $\mathcal{M}_2 = \{8, 9, 11, 22, 30, 35, 48, 49, 61, 68, 74\}$. Therefore $i_{13} = 9, i_{19} = 11$ and $i_{79} = 8$. This is not possible by applying the case $k = 73$ to $(n + 9d) \cdots (n + 81d)$. Similarly for $(i_{37}, i_{83}) = (14, 5)$, we get $i_{73} = 15$, $i_{79} = 9$ and this is excluded by applying the case $k = 73$ to $(n + 10d) \cdots (n + 82d)$. For all the remaining cases, we continue similarly to find that $\mathcal{M}_2$ is not covered by $\mathcal{P}_2$ for possible choices of i_{73} and hence they are excluded. □

10.5.10. The case $k = 89$. We have $q_1 = 79, q_2 = 89$ and $\mathcal{P}_1 = \{13, 17, 19, 23, 31, 47, 53, 71, 83\}$. Then the pairs (i_{q_1}, i_{q_2}) are given by $(16, 6), (17, 7), (18, 8), (19, 9), (20, 10), (21, 11)$. These pairs are of the form $(i + 10, i)$ with $6 \le i \le 11$.

Let $(i_{79}, i_{89}) = (16, 6)$. We see that $\mathcal{P}_1 = \{13, 17, 19, 23, 31, 47, 53, 71, 83\}$, $\mathcal{M}_1 = \{0, 1, 2, 3, 4, 10, 12, 17, 19, 24, 26, 27, 30, 33, 38, 42, 43, 44, 48, 49, 56, 57, 61, 64, 69, 72, 76, 78, 82\}$, $\mathcal{B}_1 = \{5, 7, 8, 9, 11, 13, 14, 15, 18, 20, 21, 22, 23, 25, 28, 29, 31, 32, 34, 35, 36, 37, 39, 40, 41, 45, 46, 47, 50, 51, 52, 53, 54, 55, 58, 59, 60, 62, 63, 65, 66, 67, 68, 70, 71, 73, 74, 75, 77, 79, 80, 81, 83, 84, 85, 86, 87, 88\}$, $i_{13} = 4$, $i_{17} = 10, i_{19} = 0, i_{23} = 3, i_{31} = 2$, $i_{47} = 1$ and $\{12, 24, 42\}$ is covered by $53, 71, 83$. Further $p \nmid a_i$ for $i \in \mathcal{B}_1$ and $p \in \mathcal{P}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{79, 89\}$, $p_1 = 31, p_2 = 89$, $(i_1, i_2) := (2, 6)$, $\mathcal{I} = \mathcal{B}_1$ and $\mathcal{P} = \mathcal{P}_2 := \Lambda(31, 89) \setminus \mathcal{P}_0 = \{7, 11, 41, 59, 73\}$. If $7 \nmid d$, we observe that there is at least 1 multiple of 7 among $n + (i_{13} + 13i)d$, $0 \le i \le 6$ and $\ell \le \ell_2 = \sum_{p \in \mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil - 1 = 28$. Thus in all cases, we have $\ell \le \ell_2$ and $|\mathcal{I}'| = |\mathcal{B}_1| > 2\ell_2$. Therefore the conditions of Corollary 10.3.3 are satisfied and we get $\mathcal{M} =: \mathcal{M}_2$ and $\mathcal{B} =: \mathcal{B}_2$ with $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ having *Property* $\mathfrak{H}$. We find $\mathcal{M}_2 = \{7, 11, 13, 22, 25, 29, 32, 36, 39, 40, 51, 53, 54, 60, 62, 67, 73, 74, 81, 84, 88\}$, $\mathcal{B}_2 = \{5, 8, 9, 14, 15, 18, 20, 21, 23, 28, 31, 34, 35, 37, 41, 45, 46, 47, 50, 52, 55, 58, 59, 63, 65, 66, 68, 70, 71, 75, 77, 79, 80, 83, 85, 86, 87\}$, $i_7 = 4, i_{11} = 7, i_{41} = 13$ and $\{22, 36\}$ is covered by $59, 73$. Further for $p \in \mathcal{P}_2$, $p \nmid a_i$ for $i \in \mathcal{B}_2 \setminus \{18\}$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{79, 89\}$, $p_1 = 41, p_2 = 79$, $(i_1, i_2) := (13, 16)$,

$\mathcal{I} = \mathcal{B}_2 \setminus \{18\}$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(41, 79) \setminus \mathcal{P}_0 = \{37, 43, 61, 67\}$ and $\ell = \ell_3 = \sum_{p\in\mathcal{P}_3} \lceil \frac{k}{p} \rceil = 10$. Then $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_2| - 1 > 2\ell_3$. Thus the conditions of Corollary 10.3.3 are satisfied and we have $\mathcal{M} =: \mathcal{M}_3$, $\mathcal{B} =: \mathcal{B}_3$ and $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ has *Property* $\mathfrak{H}$. We get $\mathcal{M}_3 = \{9, 21, 28, 34, 52, 58\}$, $\mathcal{B}_3 = \{5, 8, 14, 15, 20, 23, 31, 35, 37, 41, 45, 46, 47, 50, 55, 59, 63, 65, 66, 68, 70, 71, 75, 77, 79, 80, 83, 85, 86, 87\}$, $i_{37} = 21, i_{43} = 9$ and $\{28, 34\}$ is covered by $61, 67$. Therefore $p \in \{2, 3, 5, 29\}$ whenever $p|a_i$ for $i \in \mathcal{B}_3$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{79, 89\}$, $p_1 = 7, p_2 = 17$, $(i_1, i_2) := (4, 10)$, $\mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(7, 17) \setminus \mathcal{P}_0 = \{29\}$ and $\ell = \ell_4 = \lceil \frac{k}{29} \rceil = 4$. Then $|\mathcal{I}'| = |\mathcal{B}_3| - 1$ since $46 \in \mathcal{B}_3$ and $|\mathcal{B}_3| - 1 > 2\ell_3$. By Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_4$ and $\mathcal{B} =: \mathcal{B}_4$ with $(\mathcal{M}_4, \mathcal{B}_4, \mathcal{P}_4, \ell_4)$ having *Property* $\mathfrak{H}$. We find $\mathcal{M}_4 = \{8, 37, 66\}$, $\mathcal{B}_4 = \{5, 14, 15, 20, 23, 31, 35, 41, 45, 47, 50, 55, 59, 63, 65, 68, 70, 71, 75, 77, 79, 80, 83, 85, 86, 87\}$, $i_{29} = 8$ and $P(a_i) \le 5$ for $i \in \mathcal{B}_4$. Now we get a contradiction by taking $k = 6$ and $(n+47d)(n+55d)(n+63d)(n+71d)(n+79d)(n+87d) = b'y'^2$. Similarly the pair $(i_{79}, i_{89}) = (17, 7)$ is excluded by applying $k = 6$ to $(n + 48d)(n + 56d)(n + 64d)(n + 72d)(n + 80d)(n + 88d)$. For all the remaining cases, we continue similarly to find that $\mathcal{M}_3$ is not covered by $\mathcal{P}_3$ and hence they are excluded. □

10.6. Proof of Lemma 10.4.3

Assume that $Q_1 \nmid d$ and $Q_2 \nmid d$. Then, by taking mirror image (2.2.1) of (2.1.1), there is no loss of generality in assuming that $0 \le i_{Q_1} < Q_1, 0 \le i_{Q_2} \le \min(Q_2 - 1, \frac{k-1}{2})$. Further $i_{Q_2} \ge k - k'$ if $Q_2 = k$. Let $\mathcal{P}_0 = \{Q_0\}, p_1 = Q_1, p_2 = Q_2, (i_1, i_2) := (i_{Q_1}, i_{Q_2})$, $\mathcal{I} = [0, k) \cap \mathbb{Z}$ and $\mathcal{P} = \mathcal{P}_1 := \Lambda(Q_1, Q_2) \setminus \mathcal{P}_0$. Then $|\mathcal{I}'| \ge k - \lceil \frac{k}{Q_1} \rceil - \lceil \frac{k}{Q_2} \rceil$ and $\ell \le \ell_1$ where $\ell_1 = \sum_{p\in\mathcal{P}_1} \lceil \frac{k}{p} \rceil$. In fact we can take $\ell_1 = \sum_{p\in\mathcal{P}_1} \lceil \frac{k}{p} \rceil - 1$ if $(k, Q_0) = (79, 23)$ or $(k, Q_0) = (59, 29)$ with $i_7 \le 2$ by considering multiples of $13, 11$ or $19, 7, 11$, respectively.

Let $(k, Q_0) \ne (79, 73)$. Then $\ell_1 < \frac{1}{2}|\mathcal{I}'|$. We observe that $\mathfrak{i}(\mathcal{P}_0) = 0$ for $i \in \mathcal{I}'$ since $Q_0|d$ and by Corollary 10.3.3, we get $\mathcal{M} =: \mathcal{M}_1$, $\mathcal{B} =: \mathcal{B}_1$ and $(\mathcal{M}_1, \mathcal{B}_1, \mathcal{P}_1, \ell_1)$ has *Property* $\mathfrak{H}$. We now restrict to all such pairs (i_{Q_1}, i_{Q_2}) with $|\mathcal{M}_1| \le \ell_1$ and $\mathcal{M}_1$ is covered by $\mathcal{P}_1$. These pairs are given by

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

Let $(k, Q_0) = (79, 73)$ and $(Q_1, Q_2) = (53, 67)$. We apply Lemma 10.3.2 to derive that either $|\mathcal{I}_1| \le \ell_1, \mathcal{I}_1$ is covered by $\mathcal{P}_1$, $\mathfrak{i}(\mathcal{P}_1)$ is even for $i \in \mathcal{I}_2$ or $|\mathcal{I}_2| \le \ell_1, \mathcal{I}_2$ is covered by $\mathcal{P}_1$, $\mathfrak{i}(\mathcal{P}_1)$ is even for $i \in \mathcal{I}_1$. We compute $\mathcal{I}_1, \mathcal{I}_2$ and we find that both $\mathcal{I}_1$ and $\mathcal{I}_2$ are not covered by $\mathcal{P}_1$ for each pair (i_{53}, i_{67}) with $0 \le i_{53} < 53, 0 \le i_{67} \le \frac{k-1}{2}$.

Let $(k, Q_0) = (37, 29), (Q_1, Q_2) = (7, 17)$ and $(i_7, i_{17}) = (1, 2)$. Then $\mathcal{P}_1 = \{11, 13, 19, 23, 37\}$. We find that $\mathcal{M}_1 = \{3, 7, 10, 13, 14, 17, 23, 25\}$, $\mathcal{B}_1 = \{0, 4, 5, 6, 9, 11, 12, 16, 18, 20, 21, 24, 26, 27, 28, 30, 31, 32, 33, 34, 35\}$, $i_{11} = 3$, $i_{13} = 10$ and $\{7, 13, 17\}$ is covered by $19, 23, 37$. Further $p \nmid a_i$ for $p \in \mathcal{P}_1$, $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{7, 17, 29\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (3, 10)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31\}$ and $\ell = \ell_2 = \sum_{p\in\mathcal{P}_2} \lceil \frac{k}{p} \rceil = 10$. Thus $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_1| = 21 > 2\ell_2$. Then the conditions of Corollary 10.3.3 are satisfied and we have $\mathcal{M} =: \mathcal{M}_2, \mathcal{B} =: \mathcal{B}_2$ and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$. We get $\mathcal{M}_2 = \{5, 6, 16, 21, 26, 31\}$, $\mathcal{B}_2 = \{0, 4, 9, 11, 12, 18, 20, 24, 27, 28, 30, 32, 33, 34, 35\}$, $i_5 = 1$, $31|a_5$ and $5 \nmid a_{11}$. Also $P(a_i) \le 3$ for $i \in B_2$ and $P(a_{31}) = 5$. Thus $P(a_{30}a_{31} \cdots a_{35}) \le 5$ and this is excluded by the case $k = 6$. The other cases for $k = 29, 37, 47$ are excluded similarly. Each possibility is excluded by the case $k = 6$ after showing $P(a_1a_2 \cdots a_6) \le 5$ when $(k, Q_0) \in \{(29, 19), (37, 19), (37, 29), (47, 29)\}$, $(i_7, i_{17}) = (0, 0)$; $P(a_{22}a_{23} \cdots a_{27}) \le 5$ when $(k, Q_0) = (29, 19), (i_7, i_{17}) = (0, 11)$; $P(a_{30}a_{31} \cdots a_{35}) \le 5$ when $(k, Q_0) = (37, 19), (i_7, i_{17}) = (1, 2)$ and $P(a_{40}a_{41} \cdots a_{45}) \le 5$ when $(k, Q_0) = (47, 29), (i_7, i_{17}) = (4, 12)$.

Let $(k, Q_0) = (59, 29), (Q_1, Q_2) = (7, 17)$ and $(i_7, i_{17}) = (1, 1)$. Then $\mathcal{P}_1 = \{11, 13, 19, 23, 37, 47, 59\}$. We find that $\mathcal{M}_1 = \{0, 12, 14, 20, 23, 24, 27, 30, 34, 38, 39, 40, 45, 47, 48, 53, 56, 58\}$, $\mathcal{B}_1 = \{2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 16, 17, 19, 21, 25, 26, 28, 31, 32, 33, 37, 41, 42, 44, 46, 49, 51, 54, 55\}$, $i_{11} = i_{13} = i_{19} = i_{23} = 1$, $\{30, 38, 48\}$ is covered by $37, 47, 59$. Further $p \nmid a_i$ for $p \in \mathcal{P}_1$, $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{7, 17, 29\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (1, 1)$, $\mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 31, 43\}$ and $\ell =$

$\ell_2 = \sum_{p\in\mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil$. By Lemma 10.3.2, we get $M = \{6, 11, 16, 21, 31, 32, 41, 44, 46\}$, $i_5 = 1$, $31\cdot 43|a_{32}a_{44}$ and $\mathfrak{i}(\mathcal{P}_2)$ is even for $i \in B = \{2, 3, 4, 5, 7, 9, 10, 13, 17, 19, 25, 26, 28, 33, 37, 42, 49, 51, 54, 55\}$. Further for $p \in \mathcal{P}_2$, $p \nmid a_i$ for $i \in B$. Finally we apply Lemma 10.3.2 with $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{7, 17, 29\}$, $p_1 = 5, p_2 = 11$, $(i_1, i_2) := (1, 1)$, $\mathcal{I} = B$ and $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41, 53\}$. We get $M_1 = \{4, 7, 13, 25, 28, 42, 49, 54, 55\}$ which is covered by $\mathcal{P}_3$, $i_3 = 1$, $\{42, 54\}$ is covered by $\{41, 53\}$ and $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B_1 = \{2, 3, 5, 9, 10, 17, 19, 33, 37\}$. Hence $P(a_i) \le 2$ for $i \in B_1$. Since $\left(\frac{a_i}{29}\right) = \left(\frac{n}{29}\right)$ and $\left(\frac{2}{29}\right) \ne 1$, we see that $a_i = 1$ for $i \in B_1$. By taking $\mathcal{J} = B_1$, we derive that either $\mathcal{I}_5^+ = \emptyset$ or $\mathcal{I}_5^- = \emptyset$ which is a contradiction. The other case $(i_7, i_{17}) = (1, 6)$ is excluded similarly.

Let $(k, Q_0) = (71, 43), (Q_1, Q_2) = (53, 67), (i_{53}, i_{67}) = (0, 0)$. Then $\mathcal{P}_1 = \{7, 11, 13, 19, 23, 71\}$. We get $\mathcal{M}_1 = \{7, 11, 13, 14, 19, 21, 22, 23, 26, 28, 33, 35, 38, 39, 42, 43, 44, 46, 52, 55, 56, 57, 63, 65, 66, 69, 70\}$, $\mathcal{B}_1 = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 17, 18, 20, 24, 25, 27, 29, 30, 31, 32, 34, 36, 37, 40, 41, 45, 47, 48, 49, 50, 51, 54, 58, 59, 60, 61, 62, 64, 68\}$, $i_7 = i_{11} = i_{13} = i_{19} = i_{23} = 0$, $i_{71} = 43$. Further, for $p \in \mathcal{P}_1$, $p \nmid a_i$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{43, 53, 67\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (0, 0), \mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5, 17, 29, 31, 37, 47, 59, 61\}$ and $\ell = \ell_2 = \sum_{p\in\mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil$. By Lemma 10.3.2, we see that $M = \{5, 10, 15, 17, 20, 29, 30, 31, 34, 37, 40, 45, 47, 51, 58, 59, 60, 61, 62, 68\}$ is covered by $\mathcal{P}_2$, $\mathfrak{i}(\mathcal{P}_2)$ is even for $i \in B = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 25, 27, 32, 36, 41, 48, 49, 50, 54, 64\}$. We get $i_5 = i_{17} = i_{29} = i_{31} = 0$, and $\{37, 47, 59, 61\}$ is covered by $37, 47, 59, 61$. Thus $37 \cdot 47 \cdot 59 \cdot 61|a_{37}a_{47}a_{59}a_{61}$. Further $p \nmid a_i$ for $i \in B$ and $p \in \mathcal{P}_2$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{43, 53, 67\}$, $p_1 = 5, p_2 = 11$, $(i_1, i_2) := (0, 0), \mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41\}$ and $\ell = \ell_3 = \sum_{p\in\mathcal{P}_3} \left\lceil \frac{k}{p} \right\rceil$. By Lemma 10.3.2, we see that $M_1 = \{3, 6, 12, 24, 27, 41, 48, 54\}$ is covered by $\mathcal{P}_3$, $\mathfrak{i}(\mathcal{P}_3)$ is even for $i \in B_1 = \{1, 2, 4, 8, 9, 16, 18, 32, 36, 49, 64\}$. Thus $i_3 = 0$ implying $i_{41} = 0$ and $p = 2$ whenever $p|a_i$ for $i \in B_1$. By taking $\mathcal{J} = B_1$, we have $B_1 = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

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

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

Let $k = 89$, $Q_0 = 79$, $(Q_1, Q_2) = (23, 73)$, $(i_{23}, i_{73}) = (19, 15)$. Then $\mathcal{P}_1 = \{13, 19, 29, 31, 37, 47, 59, 61, 67, 79, 89\}$. We find that $\mathcal{M}_1 = \{1, 9, 10, 12, 14, 21, 23, 26, 27, 29, 30, 31, 36, 41, 49, 50, 51, 57, 59, 62, 69, 75\}$, $\mathcal{B}_1 = \{0, 2, 3, 4, 5, 6, 7, 8, 11, 13, 16, 17, 18, 20, 22, 24, 25, 28, 32, 33, 34, 35, 37, 38, 39, 40, 43, 44, 45, 46, 47, 48, 52, 53, 54, 55, 56, 58, 60, 61, 63, 64, 66, 67, 68, 70, 71, 72, 73, 74, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87\}$, $i_{13} = 10, i_{19} = 12, i_{29} = 1$, $i_{31} = 26, i_{37} = 14$ and $\{9, 21, 27, 29, 41\}$ is covered by $47, 59, 61, 67, 89$. Thus $i_{89} \in \{9, 21, 27, 29, 41\}$. Further for $p \in \mathcal{P}_1$, $p \nmid a_i$ for $i \in \mathcal{B}_1$. Now we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \{23, 73, 79\}$, $p_1 = 19, p_2 = 29$, $(i_1, i_2) := (12, 1), \mathcal{I} = \mathcal{B}_1$, $\mathcal{P} = \mathcal{P}_2 := \Lambda(19, 29) \setminus \mathcal{P}_0 = \{11, 17, 43, 53, 71\}$ and $\ell = \ell_2 = \sum_{p\in\mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 22$. Thus $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_1| > 2\ell_2$. By Corollary 10.3.3, we have $\mathcal{M} =: \mathcal{M}_2$, $\mathcal{B} =: \mathcal{B}_2$ and $(\mathcal{M}_2, \mathcal{B}_2, \mathcal{P}_2, \ell_2)$ has *Property* $\mathfrak{H}$. We get $\mathcal{M}_2 = \{0, 2, 3, 11, 17, 20, 22, 33, 35, 37, 44, 45, 54, 55, 66, 71, 77\}$, $\mathcal{B}_2 = \{4, 5, 6, 7, 8, 13, 16, 18, 24, 25, 28, 32, 34, 38, 39, 40, 43, 46, 47, 48, 52, 53, 56, 58, 60, 61, 63, 64, 67, 68, 70, 72, 73, 74, 76, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87\}$, $i_{11} = 0, i_{17} = 3, i_{43} = 2$ and $\{17, 35\}$ is covered by $53, 71$. Further $p \nmid a_i$ for $i \in \mathcal{B}_2$ and $p \in \mathcal{P}_2$. We take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \{23, 73, 79\}$, $p_1 = 11, p_2 = 13$, $(i_1, i_2) := (0, 10), \mathcal{I} = \mathcal{B}_2$, $\mathcal{P} = \mathcal{P}_3 := \Lambda(11, 13) \setminus \mathcal{P}_0 = \{5\}$ and $\ell = \ell_3 = \sum_{p\in\mathcal{P}_2} \left\lceil \frac{k}{p} \right\rceil = 18$. Thus $|\mathcal{I}'| = |\mathcal{I}| = |\mathcal{B}_2| > 2\ell_3$. Then the conditions of Corollary 10.3.3 are satisfied and we have $\mathcal{M} =: \mathcal{M}_3$, $\mathcal{B} =: \mathcal{B}_3$ with $(\mathcal{M}_3, \mathcal{B}_3, \mathcal{P}_3, \ell_3)$ having *Property* $\mathfrak{H}$. We get $\mathcal{M}_3 = \{8, 18, 28, 43, 48, 53, 58, 68, 73, 78, 83\}$, $\mathcal{B}_3 = \{4, 5, 6, 7, 13, 16, 24, 25, 32, 34, 38, 39, 40, 46, 47, 52, 56, 60, 61, 63, 64, 67, 70, 72, 74, 76, 79, 80, 81, 82, 84, 85, 86, 87\}$, $i_5 = 3$. Lastly we take $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \{23, 73, 79\}$, $p_1 = 5, p_2 = 11$, $(i_1, i_2) := (3, 0), \mathcal{I} = \mathcal{B}_3$, $\mathcal{P} = \mathcal{P}_4 := \Lambda(5, 11) \setminus \mathcal{P}_0 = \{3, 41\}$ and $\ell = \ell_4 = \sum_{p\in\mathcal{P}_4} \left\lceil \frac{k}{p} \right\rceil$. By Lemma 10.3.2, we see that $M = \{4, 6, 34, 40, 46, 47, 61, 64, 67, 76, 82, 85\}$ is covered by $\mathcal{P}_4$, $\mathfrak{i}(\mathcal{P}_4)$ is even for $i \in B = \{5, 7, 16, 24, 25, 32, 39, 52, 56, 60, 70, 72, 74, 79, 80, 81, 84, 86, 87\}$. Thus $i_3 = 1, i_{41} = 6$ and $p \in \{2, 7, 83\}$ whenever $p|a_i$ for $i \in B$. Since $79|d$, we see that $a_i \in \{1, 2, 83, 2 \cdot 83\}$ or $a_i \in \{7, 14, 7 \cdot 83, 14 \cdot 83\}$ for $i \in B$. The latter possibility is excluded since $7 \nmid (i - i')$ for all $i, i' \in B$. By taking $\mathcal{J} = B$, we have $B = \mathcal{I}_5^+ \cup \mathcal{I}_5^-$ with

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

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

10.7. Proof of Lemma 10.4.4

Let $7 \le k \le 97$ be primes. Suppose that the assumptions of Lemma 10.4.4 are satisfied. Assume that $q_1|d$ or $q_2|d$ and we shall arrive at a contradiction. We divide the proof in subsections 5.1 and 5.2

10.7.1. The cases $7 \le k \le 23$. We take $r = 3$ in (9.2.1). We may suppose that $5|d$ if $k = 7, 11$ and $11|d$ if $k = 13$. Let $5|d$. Then

$$\mathcal{B}_r \subseteq \{1, 6\} \text{ or } \mathcal{B}_r \subseteq \{2, 3\} \tag{10.7.1}$$

according as $(\frac{n}{5}) = 1$ or -1, respectively. Thus (10.7.1) holds if $k = 7, 11$. Let $11|d$. Then

$$\mathcal{B}_r \subseteq \{1, 3, 5, 15\} \text{ or } \mathcal{B}_r \subseteq \{2, 6, 10, 30\} \tag{10.7.2}$$

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

$$\mathcal{B}_r \subseteq \{1, 3, 10, 30\} \text{ or } \mathcal{B}_r \subseteq \{2, 5, 6, 15\} \tag{10.7.3}$$

according as $(\frac{n}{13}) = 1$ or -1, respectively. Thus either (10.7.2) or (10.7.3) holds if $13 \le k \le 23$.

We have

$$F(k, r) \le t_1' := \begin{cases} F'(k, 3) & \text{if } k = 7, 11 \\ F'(k, 3) - 2 & \text{if } 13 \le k < 23 \\ F'(k, 3) - 3 & \text{if } k = 23. \end{cases}$$

For the last expression, we observe that 7 and 11 together divide at most six a_i's when $k = 23$. Therefore we get from (9.2.1) that

$$\xi_r \ge k - t_1' \tag{10.7.4}$$

We divide the proof into 4 cases.

Case I. Let $2 \nmid d$ and $3 \nmid d$. From (10.7.1), (10.7.2), (10.7.3) and Corollary 10.4.1, we get

$$\xi_r \le t_1 := \begin{cases} \max(f_4(k, 1, 0) + f_4(k, 6, 0), f_4(k, 2, 0) + f_4(k, 3, 0)) + \lceil \frac{k}{4} \rceil & \text{if } k = 7, 11, \\ f_4(k, 1, 0) + f_4(k, 3, 0) + f_4(k, 5, 0) + f_4(k, 15, 0) + \lceil \frac{k}{4} \rceil & \text{if } k > 11 \end{cases}$$

since $f_4(k, a, \delta)$ is non-increasing function of a and $\sum_{a \in R} \nu_e(a) \le \lceil \frac{k}{4} \rceil$. We check that $t_1 + t_1' < k$ contradicting (10.7.4).

Thus we have either $2|d$ or $3|d$. Let $k = 7, 11$. If $2|d$, then $\mathcal{B}_r \subseteq \{1\}$ or $\mathcal{B}_r \subseteq \{3\}$. If $3|d$, we have $\mathcal{B}_r \subseteq \{1\}$ or $\mathcal{B}_r \subseteq \{2\}$. By Lemma 9.5.3, we get $\xi_r \le \frac{k-1}{2}$. We check that $\frac{k-1}{2} + t_1' < k$ contradicting (10.7.4). From now on, we may also that suppose that $13 \le k \le 23$.

Case II. Let $2|d$ and $3 \nmid d$. Then $\mathcal{B}_r \subseteq \{1, 3, 5, 15\}$ if $11|d$ and $\mathcal{B}_r \subseteq \{1, 3\}$ or $\mathcal{B}_r \subseteq \{5, 15\}$ if $13|d$. Let $2||d$. From Corollary 10.4.1 with $\delta = 1$, we get

$$\xi_r \le F_1(k, 1, 1) + F_1(k, 3, 1) + F_1(k, 5, 1) + F_1(k, 15, 1) =: t_2.$$

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

$$\xi_r \le F_1(k, 1, 2) + F_1(k, 5, 2) =: t_3.$$

by Corollary 10.4.1 with $\delta = 2$. Let $8|d$. Then $a_i \equiv n(\text{mod } 8)$ and Corollary 10.4.1 with $\delta = 3$ imply

$$\xi_r \le F_1(k, 1, 3) =: t_4.$$

Thus $\xi_r \le$max(t_2, t_3, t_4). This contradicts (10.7.4).

Case III. Let $2 \nmid d$ and $3|d$. From $a_i \equiv n(\text{mod } 3)$, we see that either $S = \emptyset$ or $S = \{1\}, \{2\}, \{5\}$ or $\{10\}$ if $11|d$ and $\mathcal{B}_r \subseteq \{1, 10\}$ or $\mathcal{B}_r \subseteq \{2, 5\}$ if $13|d$. By Corollary 10.4.1, we get

$$\xi_r \le F_1(k, 1, 0) + F_1(k, 5, 0),$$

contradicting (10.7.4).

Case IV. Let $2|d$ and $3|d$. Then $\mathcal{B}_r \subseteq \{1\}, \{5\}$. By Lemma 9.5.3, we get $\xi_r \leq \frac{k-1}{2}$. We check that $\frac{k-1}{2} + t'_1 < k$. This contradicts (10.7.4).

10.7.2. The cases $k \geq 29$. Let $29 \leq k \leq 59$ and $19|d$. Then by Lemma 10.4.3 with $Q_0 = 19$, we get $7|d$ or $17|d$. Thus we get a prime pair $(Q, Q') = (7, 19)$ or $(Q, Q') = (17, 19)$ such that $QQ'|d$. Similarly we get $(Q, Q') = (7, 29)$ or $(Q, Q') = (17, 29)$ with $QQ'|d$ when $31 \leq k \leq 59$ and $29|d$. Let $k = 71$. Then we have either $43|d, 67|d$ or $43|d, 67 \nmid d$ or $43 \nmid d, 67|d$. We get prime pair $(Q, Q') = (43, 67)$ with $QQ'|d$ if $43|d, 67|d$. If $43|d, 67 \nmid d$, we get from Lemma 10.4.3 with $Q_0 = 43$ that $53|d$ and we take $(Q, Q') = (43, 53)$ such that $QQ'|d$. If $43 \nmid d, 67|d$, we get from Lemma 10.4.3 with $Q_0 = 67$ that $53|d$ and we take $(Q, Q') = (53, 67)$ such that $QQ'|d$. Similarly we get prime pairs (Q, Q') with $QQ'|d$ for each $61 \leq k \leq 97$ are given in the table below. For $r \leq 7$, we see that

$$F(k, r) \leq \sum_{\substack{p > p_r \\ p \neq Q, Q'}} \lceil \frac{k}{p} \rceil \leq F'(k, r) - t'_2$$

where $t'_2 = 2, 4, 7$ according as $29 \leq k \leq 61, 61 < k < 97, k = 97$, respectively. Therefore we get from (9.2.1) that

$$\xi_r \geq k + t'_2 - F'(k, r). \tag{10.7.5}$$

Case I. Let $2 \nmid d$ and $3 \nmid d$. We take $r = 5$ if $k = 71$, $(Q, Q') = (43, 67)$ and $r = 4$ otherwise. Then $\mathcal{B}_r \subseteq \mathcal{S}_j(1, r) = \mathcal{S}_j(0, 1, Q, Q', r)$ for some some j with $1 \leq j \leq 4$ where $\mathcal{S}_j(1, r)$ is given by (9.2.7). For each value of k, we give below a table for (Q, Q') and $\mathcal{S}_j(1, r)$ for $1 \leq j \leq 4$.

k	(Q, Q')	$\mathcal{S}_1(1, r), \mathcal{S}_2(1, r), \mathcal{S}_3(1, r), \mathcal{S}_4(1, r)$
$29 \leq k \leq 59$	$(7, 19), (7, 29)$	$\{1, 30\}, \{2, 15\}, \{3, 10\}, \{5, 6\}$
$29 \leq k \leq 59$	$(17, 19), (17, 29)$	$\{1, 30, 35, 42\}, \{2, 15, 21, 70\}, \{3, 10, 14, 105\}, \{5, 6, 7, 210\}$
61	$(11, 59)$	$\{1, 3, 5, 15\}, \{2, 6, 10, 30\}, \{7, 21, 35, 105\}, \{14, 42, 70, 210\}$
$67, 71$	$(43, 53)$	$\{1, 6, 10, 15\}, \{2, 3, 5, 30\}, \{7, 42, 70, 105\}, \{14, 21, 35, 210\}$
71	$(43, 67)$	See (10.7.6)
71	$(53, 67)$	$\{1, 6, 10, 15\}, \{2, 3, 5, 30\}, \{7, 42, 70, 105\}, \{14, 21, 35, 210\}$
73	$(23, 53)$	$\{1, 6, 70, 105\}, \{2, 3, 35, 210\}, \{5, 14, 21, 30\}, \{7, 10, 15, 42\}$
73	$(23, 67)$	$\{1, 6, 35, 210\}, \{2, 3, 70, 105\}, \{5, 7, 30, 42\}, \{10, 14, 15, 21\}$
79	$(23, 53), (53, 73)$	$\{1, 6, 70, 105\}, \{2, 3, 35, 210\}, \{5, 14, 21, 30\}, \{7, 10, 15, 42\}$
79	$(23, 67), (67, 73)$	$\{1, 6, 35, 210\}, \{2, 3, 70, 105\}, \{5, 7, 30, 42\}, \{10, 14, 15, 21\}$
83	$(23, 37), (37, 73)$	$\{1, 3, 70, 210\}, \{2, 6, 35, 105\}, \{5, 14, 15, 42\}, \{7, 10, 21, 30\}$
89	$(23, 79), (73, 79)$	$\{1, 2, 105, 210\}, \{3, 6, 35, 70\}, \{5, 10, 21, 42\}, \{7, 14, 15, 30\}$
97	$(23, 37), (23, 83)$	$\{1, 3, 70, 210\}, \{2, 6, 35, 105\}, \{5, 14, 15, 42\}, \{7, 10, 21, 30\}$

For $k = 71$, $(Q, Q') = (43, 67)$, we get from $r = 5$ that

(10.7.6)

$$\mathcal{S}_1(1, r) = \{1, 6, 10, 14, 15, 21, 35, 210\}, \mathcal{S}_2(1, r) = \{2, 3, 5, 7, 30, 42, 70, 105\}$$

$$\mathcal{S}_3(1, r) = \{11, 66, 110, 154, 165, 231, 385, 2310\}, \mathcal{S}_4(1, r) = \{22, 33, 55, 77, 330, 462, 770, 1155\}.$$

From Corollary 10.4.1, we get

$$\xi_r \leq t_5 := \max_{1 \leq j \leq 4} \{ \sum_{s \in \mathcal{S}_j(1, r)} F_1(k, s, 0).$$

We check that $t_5 + F'(k, r) - t'_2 < k$ contradicting (10.7.5).

Case II. Let $2|d$ and $3 \nmid d$. We take $r = 4$ for $2||d, 4||d$ and $r = 5$ for $8|d$. Let $2||d$. Then $\mathcal{B}_r \subseteq \{1, 3, 5, 7, 15, 21, 35, 105\} =: \mathcal{B}^{(2)}$. From Corollary 10.4.1 with $\delta = 1$, we get

$$\xi_r \leq \sum_{b \in \mathcal{B}^{(2)}} F_1(k, b, 1) =: t_6$$

Let $4||d$. Then we see that either $\mathcal{B}_r \subseteq \{1,5,21,105\} =: \mathcal{B}^{(41)}$ or $\mathcal{B}_r \subseteq \{3,7,15,35\} =: \mathcal{B}^{(43)}$. From Corollary 10.4.1 with $\delta = 2$, we get

$$\xi_r \le \max_{i=1,3} \sum_{b \in \mathcal{B}^{(4i)}} F_1(k,b,2) =: t_7.$$

Hence, if $8 \nmid d$, then $\xi_r \le$max(t_6,t_7). We obtain $\max(t_6,t_7) + F'(k,r) - t_2' < k$. This contradicts (10.7.5).

Let $8|d$. Then we see from $a_i \equiv n(\text{mod } 8)$ that $\mathcal{B}_r \subseteq \{1,33,105,385\} =: \mathcal{B}^{(81)}$ or $\mathcal{B}_r \subseteq \{3,11,35,1155\} =: \mathcal{B}^{(83)}$ or $\mathcal{B}_r \subseteq \{5,21,77,165\} =: \mathcal{B}^{(85)}$ or $\mathcal{B}_r \subseteq \{7,15,55,231\} =: \mathcal{B}^{(87)}$. Then

$$\xi_r \le \max_{i=1,3,5,7} \sum_{b \in \mathcal{B}^{(8i)}} F_1(k,b,3) =: t_8.$$

by Corollary 10.4.1 with $\delta = 3$. We check that $t_8 + F'(k,r) - t_2' < k$ contradicting (10.7.5).

Case III. Let $2 \nmid d$ and $3|d$. We take $r = 5$. Then by modulo 3, we get either $\mathcal{B}_r \subseteq \{1,7,10,22,55,70, 154,385\} =: \mathcal{B}^{(31)}$ or $\mathcal{B}_r \subseteq \{2,5,11,14,35,77,110,770\} =: \mathcal{B}^{(32)}$. By Corollary 10.4.1, we get

$$\xi_r \le \max_{i=1,2} \sum_{b \in \mathcal{B}^{(3i)}} F_1(k,b,0) =: t_9.$$

This together with (10.7.5) implies $t_9 + F'(k,5) - t_2' \ge k$. This is contradiction.

Case IV. Let $2|d$ and $3|d$. Let $2||d$. We take $r = 4$. Then we see that either $\mathcal{B}_r \subseteq \{1,7\}$ or $\mathcal{B}_r \subseteq \{5,35\}$. By Corollary 10.4.1, we get $\xi_r \le F_1(k,1,1) + F_1(k,7,1)$ which contradicts (10.7.5).

Let $4||d$. We take $r = 6$. From $a_i \equiv n(\text{mod } 12)$, we see that

$$\mathcal{B}_r \subseteq \mathcal{B}' \in \mathfrak{B} := \{\{1,13,385,5005\},\{5,65,77,1001\},\{7,55,91,715\},\{11,35,143,455\}\}.$$

Then

$$\xi_r \le \max_{\mathcal{B}' \in \mathfrak{B}} \sum_{b \in \mathcal{B}'} F_1(k,b,2)$$

contradicting (10.7.5).

Let $8|d$. We take $r = 7$. From $a_i \equiv n(\text{mod } 24)$, we see that $\mathcal{B}_r \subseteq \mathcal{B}' = \{1,385,1105,17017\}$ or $\mathcal{B}_r \subseteq \mathcal{B}'' \in \mathfrak{B}_1$ where $\mathfrak{B}_1$ is the union of sets

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

Let $\mathcal{B}_r \subseteq \mathcal{B}'' \in \mathfrak{B}_1$. Then

$$\xi_r \le \max_{\mathcal{B}'' \in \mathfrak{B}_1} \sum_{b \in \mathcal{B}''} F_1(k,b,3) =: t_{10}$$

by Corollary 10.4.1. Let $\mathcal{B}_r \subseteq \mathcal{B}'$. By Lemma 9.5.3, we get $\nu(1) \le \frac{k-1}{2}$. This together with $\nu(1105) + \nu(17017) \le 1$ by $13 \cdot 17|\gcd(1105,17017)$ and $\nu(385) \le 1$ by Corollary 10.4.1 gives $\xi_r \le \frac{k-1}{2} + 2$. Therefore $\xi_r \le$max$(t_{10}, \frac{k-1}{2} + 2)$. Now we get a contradiction from (10.7.5). □

10.8. Proof of Theorem 10.1.1

Let $k = 7$. By the case $k = 6$, we may assume that $7 \nmid d$. Now the assertion follows from Lemmas 10.4.4 and 10.4.2. Let $k = 8$. Then by applying the case $k = 7$ twice to $n(n+d)\cdots(n+6d) = b'y'^2$ and $(n+d)\cdots(n+7d) = b''y''^2$, we get

$$(a_0,\cdots,a_6),(a_1,\cdots,a_7) \in \{(2,3,1,5,6,7,2),(3,1,5,6,7,2,1),(1,5,6,7,2,1,10),$$
$$(2,7,6,5,1,3,2),(1,2,7,6,5,1,3),(10,1,2,7,6,5,1)\}.$$

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

Let $k \geq 11$ and $k' < k$ be consecutive primes. We suppose that Theorem 10.1.1 is valid with k replaced by k'. Let $k|d$. Then $\left(\frac{a_i}{k}\right) = \left(\frac{n}{k}\right)$ for all $0 \leq i < k$. By applying the case $k = k'$ to $n(n+d)\cdots(n+(k'-1)d) = b'y'^2$ with $P(b') \leq k'$, we get $k' \leq 23$ and $1, 2, 3, 5 \in \{a_0, a_1, a_2, \cdots, a_{k'-1}\}$ in view of (2.2.2) and (2.2.3). Therefore $\left(\frac{2}{k}\right) = \left(\frac{3}{k}\right) = \left(\frac{5}{k}\right) = 1$ which is not possible.

Thus we may assume that $k \nmid d$ and $k|n+id$ for some $0 \leq i \leq \frac{k-1}{2}$ by considering the mirror image (2.2.1) of (2.1.1) whenever Theorem 10.1.1 holds at k'. We shall use this assertion without reference in the proof of Theorem 10.1.1.

Let $k = 11$. By Lemmas 10.4.4 and 10.4.2, we see that $11|n+id$ for $0 \leq i \leq 3$. If $11|n$, the assertion follows by the case $k = 10$. Let $11|n+d$. We consider $(n+2d)\cdots(n+10d) = b'y'^2$ with $P(b') \leq 7$ and the case $k = 9$ to get $(a_2, a_3, \cdots, a_{10}) \in \{(2, 3, 1, 5, 6, 7, 2, 1, 10), (10, 1, 2, 7$
$, 6, 5, \ 1, 3, 2)\}$. The first possibility is excluded since $1 = \left(\frac{14}{11}\right) = \left(\frac{a_2a_7}{11}\right) = \left(\frac{1\cdot 6}{11}\right) = -1$. For the second possibility, we observe $P(a_0) \leq 5$ since $\gcd(a_0, 7\cdot 11) = 1$ and this is excluded by the case $k = 6$ applied to $n(n+2d)(n+4d)(n+6d)(n+8d)(n+10d)$. Let $11|n+2d$. Then by the case $k = 8$, we have $(a_3, a_4, \cdots, a_{10}) \in \{(2, 3, 1, 5, 6, 7, 2, 1), (3, 1, 5, 6, 7, 2, 1, 10), (1, 2, 7, 6, 5, 1, 3, 2),$
$(10, 1, 2, 7, 6, 5, 1, 3)\}$. The first three possibilities are excluded by considering the values of Legendre symbol mod 11 at a_3, a_8; a_3, a_4 and a_3, a_5, respectively. If the last possibility holds, then $a_0 = 1$ since $\gcd(a_0, 2\cdot 3\cdot 5\cdot 7\cdot 11) = 1$ and this is not possible since $1 = \left(\frac{a_0a_4}{11}\right) = \left(\frac{(-2)2}{11}\right) = -1$. Let $11|n+3d$. We consider $(n+4d)\cdots(n+10d) = b'y'^2$ with $P(b') \leq 7$ and the case $k = 7$ to get $(a_4, \cdots, a_{10}) \in \{(2, 3, 1, 5, 6, 7, 2), (3, 1, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, 1, 10), (2, 7, 6, 5, 1, 3, 2),$
$(1, 2, 7, 6, 5, 1, 3), (10, 1, 2, 7, 6, 5, 1)\}$ which is not possible as above. This completes the proof for $k = 11$. The assertion for $k = 12$ follows from that of $k = 11$.

Let $k = 13$. Then the assertion follows from Lemmas 10.4.4, 10.4.2 and the case $k = 11$. Let $k = 14$. By applying $k = 13$ to $n(n+d)\cdots(n+12d) = b'y'^2$ and $(n+d)\cdots(n+13) = b''y''^2$, we get the assertion. Let $k = 15$. Then applying $k = 14$ both to $n(n+d)\cdots(n+13d)$ and $(n+d)\cdots(n+14d)$ gives the result. Now $k = 16$ follows from the case $k = 15$.

Let $k = 17$. Then $17|n+2d$ or $17|n+3d$ by Lemmas 10.4.4, 10.4.2 and the case $k = 15$. Let $17|n+2d$. Then by applying the case $k = 14$ to $(n+3d)\cdots(n+16d) = b'y'^2$ with $P(b') \leq 13$, we get $(a_3, a_4, \cdots, a_{16}) \in \{(3, 1, \cdots, 15, 1), (1, 15, \cdots, 1, 3)\}$. The first possibility is excluded by Legendre symbol mod 17 at a_3, a_4. For the second, we observe that $\gcd(a_1, 7\cdot 11\cdot 13\cdot 17) = 1$ which is not possible by the case $k = 6$ applied to $(n+d)(n+4d)(n+7d)(n+10d)(n+13d)(n+16d)$. Let $17|n+3d$. By considering $(n+4d)\cdots(n+16d) = b'y'^2$ with $P(b') \leq 13$, it follows from the case $k = 13$ that $(a_4, \cdots, a_{16}) \in \{(3, 1, \cdots, 14, 15), (1, 5, \cdots, 15, 1), (15, 14, \cdots, 1, 3), (1, 15, \cdots, 5, 1)\}$. The first three possibilities are excluded by considering Legendre symbol mod 17 at a_4, a_5. If the last possibility holds, we observe that $a_1 = 1$ since $\gcd(a_1, \prod_{p\leq 17} p) = 1$ and then $1 = \left(\frac{a_1a_4}{17}\right) = \left(\frac{(-6)(-3)}{17}\right) = -1$, a contradiction. The assertion for $k = 18$ follows from that of $k = 17$.

Let $k = 19$. Then the assertion follows from Lemmas 10.4.4, 10.4.2 and the case $k = 17$. By applying $k = 19$ twice to $n(n+d)\cdots(n+18d)$ and $(n+d)\cdots(n+18d)(n+19d)$, the assertion for $k = 20$ follows and this implies the cases $k = 21, 22$.

Let $k = 23$. We see from Lemmas 10.4.4, 10.4.2 and the case $k = 20$ that $23|n+3d$. We consider $k = 19$ and $(n+4d)\cdots(n+22d) = b'y'^2$ with $P(b') \leq 19$ to get $(a_4, a_5, \cdots, a_{22}) = (1, 5, \cdots, 21, 22)$ or $(22, 21, \cdots, 5, 1)$. By considering the values of Legendre symbol mod 23 at a_4 and a_5, we may assume the second possibility. Now $P(a_2) \leq 11$ and this is not possible by the case $k = 11$ applied to $(n+2d)(n+4d)\cdots(n+22d)$. Let $k = 24$. We get $(a_0, a_1, \cdots, a_{23}) = (5, 6, \cdots, 3, 7), (7, 3, \cdots, 6, 5)$ by considering $k = 23$ both to $n(n+d)\cdots(n+22d)$ and $(n+d)\cdots(n+23d)$. Further the assertion for $25 \leq k \leq 28$ follows from $k = 24$.

Let $k \geq 29$. First we consider $k = 29$. We see from Lemmas 10.4.4, 10.4.2 and the case $k = 25$ that $29|n+4d$ or $29|n+5d$. Let $29|n+4d$. Then considering $k = 24$ and $(n+5d)(n+6d)\cdots(n+28d)$, we get $(a_5, a_6, \cdots, a_{28}) = (5, 6, \cdots, 3, 7)$ or $(7, 3, \cdots, 6, 5)$. By observing $1 = \left(\frac{30}{29}\right) = \left(\frac{a_5a_6}{29}\right) = \left(\frac{1\cdot 2}{29}\right) = -1$, we may assume the second possibility. Then $a_1 = 1$ implying $1 = \left(\frac{a_2a_8}{29}\right) = \left(\frac{(-2)4}{29}\right) = -1$, a contradiction. Let $29|n+5d$. Now by considering $k = 23$ and $(n+6d)\cdots(n+28d)$, we get $(a_6, a_7, \cdots, a_{28}) \in \{(5, 6, \cdots, 26, 3), (6, 7, \cdots, 3, 7), (3, 26, \cdots, 6, 5),$

$(7, 3, \cdots, 7, 6)\}$. Then we may restrict to the last possibility by considering the Legendre symbol mod 29 at the first two entries in the remaining possibilities. It follows that $a_3 = 1$ implying $1 = \left(\frac{a_3 a_9}{29}\right) = \left(\frac{(-2)4}{29}\right) = -1$, a contradiction. This completes the proof for $k = 29$. We now proceed by induction. By Lemmas 10.4.4 and 10.4.2, the assertion follows for all primes k. Now Lemma 9.1.1 completes the proof of Theorem 10.1.1. □

10.9. Proof of Theorem 2.1.1

Observe that for all tuples in (2.2.2) and (2.2.3), the product of the a_i's is not a square. Hence, by Theorem 10.1.1, we may assume that $101 \le k \le 109$. Assume (2.1.1) with $b = 1$. Then $\mathrm{ord}_p(a_0 a_1 \cdots a_{k-1})$ is even for each prime p. Let $101 \le k \le 105$. Then $P(a_4 a_5 \cdots a_{100}) \le 97$. Now the assertion follows from Theorem 10.1.1 by considering $(n + 4d) \cdots (n + 100d)$ and $k = 97$. Let $k = 106, 107$. Then $P(a_4 a_5 \cdots a_{102}) \le 101$. We may suppose that $P(a_4 a_5) = 101$ or $P(a_{101} a_{102}) = 101$ otherwise the assertion follows by the case $k = 99$ in Theorem 10.1.1. Let $P(a_4 a_5) = 101$. Then $P(a_6 \cdots a_{102}) \le 97$ and the assertion follows by $k = 97$ in Theorem 10.1.1. This is also the case when $P(a_{101} a_{102}) = 101$ since $P(a_4 \cdots a_{100}) \le 97$ in this case. Let $k = 108, 109$. Then $P(a_6 \cdots a_{102}) \le 101$. Thus either $P(a_6 a_7) = 101$ or $P(a_{101} a_{102}) = 101$. Let $P(a_6 a_7) = 101$. Then $P(a_8 \cdots a_{102}) \le 97$. We may assume that $97 | a_8 a_9 a_{10} a_{11}$ or $97 | a_{97} \cdots a_{101} a_{102}$. Let $97 | a_8 a_9 a_{10} a_{11}$. Then $P(a_{12} a_{13} \cdots a_{102}) \le 89$ and the assertion follows by the case $k = 91$ of Theorem 10.1.1. Let $97 | a_{97} \cdots a_{102}$. Then $P(a_8 a_9 \cdots a_{96}) \le 89$ and the assertion follows from the case $k = 89$ of Theorem 10.1.1. When $P(a_{101} a_{102}) = 101$, we argue as above to get the assertion. □

CHAPTER 11

Equation (2.1.1) with with $\omega(d) \le 6$ or $d \le 10^{10}$: Proof of Theorems 2.3.1, 2.4.1, 2.5.1, 2.5.2, 2.5.3

In this chapter, we prove Theorems 2.3.1, 2.4.1, 2.5.1, 2.5.2 and 2.5.3. From now on, we take $t = k$. Thus $b_j = a_{j-1}, B_j = A_{j-1}, y_j = x_{j-1}$ and $Y_j = X_{j-1}$ for $1 \le j \le k$ in (9.1.2) and (9.1.3).

By using Theorem 10.1.1, we take $k > 100$. As in [**76**], the proof of our theorems depend on showing that the upper bound and lower bound for $n + (k-1)d$ are not consistent whenever it is possible to find a non-degenerate double pair. A lower bound for $n + (k-1)d$ is obtained by using lemmas stated in Section 9.4 and Lemma 11.1.3. Further by using the lemmas stated in Section 9.3, we give an upper bound for $n + (k-1)d$ whenever it is possible to find a non-degenerate double pair. This is always the case whenever $k - |R| \ge 2^{\omega(d)-\theta}$. If we do not have this, we use Lemmas 9.3.13 and 11.1.2 depending on an idea of Erdős to give an upper bound for k. Thus there are only finitely many possibilities for k and we use counting arguments given in Section 9.2 and computational lemmas in Section 11.1 to exclude these possibilities. For example, we show in Lemma 11.1.1 that k is large whenever d is divisible by two small primes. This is very useful in our proofs and increases considerably a lower bound for d in Theorem 2.4.1.

11.1. Computational Lemmas

Lemma 11.1.1. *Let* $k \ge 101$. *Assume* (2.1.1).
(*a*) *Let d be odd and $p < q$ be primes such that $pq|d$ with $p \le 19, q \le 47$. Then $k \ge 1733$.*
(*b*) *Let d be odd and $p < q$ be primes such that $pq|d$ with $23 \le p < q \le 43, (p,q) \ne (31,41)$. Then $k \ge 1087$.*
(*c*) *Let d be even such that $p|d$ with $3 \le p \le 47$. Then $k \ge 1801$.*

Proof. We shall use the notation and results of Section 8.2 without reference. By Lemma 9.1.1, it suffices to prove Lemma 11.1.1 when k is a prime. Let P_0 be the largest prime $\le k$ such that $P_0 \nmid d$. Then (2.1.1) holds at $k = P_0$. Therefore $P_0 \ge 101$ by Theorem 10.1.1 with $k = 97$. Thus there is no loss of generality in assuming that $k \nmid d$ for the proof of Lemma 11.1.1.
(*a*) Let d be odd and p, q be as in (*a*). Assume $k < 1733$. It suffices to consider 4 cases, viz (*i*) $5 < p < q, 3 \nmid d, 5 \nmid d$; (*ii*) $p = 3, q > 5, 5 \nmid d$; (*iii*) $p = 5, q > 5, 3 \nmid d$ and (*iv*) $p = 3, q = 5$. We take $r \ge 7$. We see that $\mathcal{B}_r$ is contained in one of the four sets $\mathcal{S}_\mu = \mathcal{S}_\mu(1,r)$ with $1 \le \mu \le 4$. Let $\mathcal{S}'_\mu = \{s \in \mathcal{S}_\mu : s < 2000\}$ with $1 \le \mu \le 4$. We have $\nu(s) \le F_0(k,s,0)$ by Lemma 9.5.2. Further $\nu(s) \le 1$ for $s \ge k$ and hence for $s \in \mathcal{S}_\mu \setminus \mathcal{S}'_\mu$. Observe that $1 \in \mathcal{S}'_1 \subseteq \mathcal{S}_1$.

Assume that $1 \notin R$ in the case (*iv*). For the case (*i*), we take $r = 7$ for $101 \le k < 1087$ and $r = 8$ for $1087 \le k < 1733$. For all other cases, we take $r = 7$ for $101 \le k < 941$, $r = 8$ for $941 \le k < 1297$ and $r = 9$ for $1297 \le k < 1733$. Then $\xi_r \le \max \sum_{s \in \mathcal{S}_\mu} \nu(s) \le \max \left(g_{p,q} - |\mathcal{S}'_\mu| + \sum_{s \in \mathcal{S}'_\mu} F(k,s,0) \right) \le g_{p,q} + \max \sum_{s \in \mathcal{S}'_\mu} (F_0(k,s,0) - 1) =: \tilde{\xi_r}$ where the maximum is taken over $1 \le \mu \le 4$ and we remove 1 from $\mathcal{S}'_1 \subseteq \mathcal{S}_1$ when the case (*iv*) holds. We now check that

$$k - F'(k,r) - \tilde{\xi_r} > \begin{cases} 0 & \text{if } p < q \le p_r \\ -\left\lceil \frac{k}{q} \right\rceil & \text{if } p \le \mathfrak{p}_r < q \\ -\left\lceil \frac{k}{p} \right\rceil - \left\lceil \frac{k}{q} \right\rceil & \text{if } \mathfrak{p}_r < p < q. \end{cases} \tag{11.1.1}$$

This contradicts (9.2.1) by using the estimates for $g_{p,q}$ and $\tilde{\xi_r} \ge \xi_r$.

Thus it remains to consider (iv) with $1 \in R$. Then $\left(\frac{a_i}{3}\right) = \left(\frac{a_i}{5}\right) = 1$ for all $a_i \in R$. Suppose that $p' \nmid d$ for some prime $p' \in \mathcal{P} = \{7, 11, 13\}$. We take $r = 9$. We have $\mathcal{B}_r \subseteq \mathcal{S}_1$. Further $|\mathcal{S}_1| = 32$ and $\mathcal{S}_1' = \{1, 19, 34, 46, 91, 154, 286, 391, 646, 874, 1309, 1729, 1771\}$. We get from (9.5.1) that $\nu_o(a) \le \min(f_0(k,a,0), f_1(k,a,p',1,0)) \le \min(f_0(k,a,0), \max_{p' \in \mathcal{P}}\{f_1(k,a,p',1,0)\}) := G_1(k,a)$. Similarly we get from (9.5.2) that $\nu_e(a) \le$min$(g_0(k,a,2), \max_{p' \in \mathcal{P}}\{g_1(k,a,p',1,0)\} := G_2(k,a)$. Let $G(k,a) = 1$ if $k \le a$ and $G(k,a) = G_1(k,a) + G_2(k,a)$ if $k > a$. Then $\nu(a) \le G(k,a)$ implying $\xi_r \le 32 + \sum_{s \in \mathcal{S}_1'}(G(k,s) - 1) =: \tilde{\xi_r}$ as above. We check that

$$k - F'(k,r) - \tilde{\xi_r} > 0. \tag{11.1.2}$$

This contradicts (9.2.1). Thus $p'|d$ for each prime $p \in \mathcal{P}$. Now we take $r = 14$. Since $1 \in R$, we have $\left(\frac{a_i}{p}\right) = 1$ for all $a_i \in R$ and for each p with $3 \le p \le 13$. Therefore $\mathcal{B}_r \subseteq \{s \in \mathcal{S}(r) : \left(\frac{s}{p}\right) = 1, 3 \le p \le 13\} = \{1, 1054\} \cup \mathcal{S}''$ where $|\mathcal{S}''| = 14$ and $s > 2000$ for each $s \in \mathcal{S}''$. Hence $\xi_r \le \nu(1) + \nu(1054) + 14 \le \nu(1) + 16$ since $\nu(1054) \le 2$ by Lemma 9.5.2. From (9.5.1) and (9.5.2) with $\mu = 3$, we get $\nu(1) \le f_0(k,1,0) + g_0(k,1,3)$. Therefore $\xi_r \le f_0(k,1,0) + g_0(k,1,3) + 16 =: \tilde{\xi_r}$ and we compute that (11.1.2) holds contradicting (9.2.1).

(b) Let d be odd and p, q be as in (b). Assume $k < 1013$. By (a), we may assume that $3 \nmid d, 5 \nmid d$. We continue the proof as above in the case (i) of (a). We take $r = 7$ and check that $k - F'(k,r) - \tilde{\xi_r} + \lceil \frac{k}{p} \rceil + \lceil \frac{k}{q} \rceil > 0$. This contradicts (9.2.1).

(c) Let d be even and p be as in (c). Assume $k < 1801$. For any set W of squarefree integers, let $W' = W'(\delta) = \{s \in W : s < \frac{2000}{2^{3-\delta}}\}$. We consider four cases, viz (i) $p > 5, 3 \nmid d, 5 \nmid d$; (ii) $p = 5, 3 \nmid d$; (iii) $p = 3, 5 \nmid d$ and (iv) $15|d$. We take $r \ge 7$. Assume that $(i), (ii)$ or (iii) holds. Then from (9.2.7) with $p = q$, we get 2^δ sets $U_\mu, 1 \le \mu \le 2^\delta$ given by $\mathcal{S}_1(n', r), \mathcal{S}_4(n', r)$. Without loss of generality, we put $\mathcal{S}_1(1, r) = U_1$. Further $|U_\mu| \le g_p$ for $1 \le \mu \le 2^\delta$. Assume (iv). We take $p = 3, q = 5$ in (9.2.7). We get $2^{\delta+1}$ sets $V_\mu, 1 \le \mu \le 2^{\delta+1}$ given by $\mathcal{S}_j(n', r), 1 \le j \le 4$ and we put $\mathcal{S}_1(1, r) = V_1$. Further $|V_\mu| \le 2^{r-\delta-4}$ for $1 \le \mu \le 2^{\delta+1}$. We define g' by $g' = 2^{r-\delta-4}$ if (iv) holds and $g' = g_p$ otherwise. Further let W_μ with $1 \le \mu \le 2^{\delta+1}$ be given by $W_\mu = V_\mu$ if (iv) holds and $W_\mu = U_\mu$ for $1 \le \mu \le 2^\delta$, $W_\mu = \emptyset$ for $\mu > 2^\delta$ if $(i), (ii)$ or (iii) holds. We see from Lemma 9.5.2 that $\nu(s) \le F_0(k, s, \delta)$ and $\nu(s) \le 1$ for $s \in W_\mu \setminus W_\mu'$. Observe that $1 \in W_1' \subseteq W_1$.

Assume that $1 \notin R$ in the cases $(ii), (iii)$ or (iv). We take $r = 8$ for $101 \le k \le 941$, $r = 9$ for $941 < k \le 1373$ and $r = 10$ for $1373 < k < 1801$ in the case (i) with $8|d$. For all other cases, we take $r = 7$ for $101 \le k \le 941$, $r = 8$ for $941 < k \le 1373$ and $r = 9$ for $1373 < k < 1801$. Then $\xi_r \le \max \sum_{s \in W_\mu} F(k, s, \delta) \le g' + \max \sum_{s \in W_\mu'} (F_0(k, s, \delta) - 1) =: \tilde{\xi_r}$ where maximum is taken over $1 \le \mu \le 2^{\delta+1}$ and we remove 1 from $W_1' \subseteq W_1$ when $(ii), (iii)$ or (iv) holds. We check that

$$k - F'(k,r) - \tilde{\xi_r} > \begin{cases} -\lceil \frac{k}{p} \rceil & \text{if } (i) \text{ holds with } p > p_r \\ 0 & \text{otherwise.} \end{cases}$$

This contradicts (9.2.1).

Thus it remains to consider the cases $(ii), (iii)$ or (iv) and $1 \in R$. Then $a_i \equiv 1 (\text{mod } 2^\delta)$ and $\left(\frac{a_i}{p}\right) = 1$ for all $p|d$ whenever $a_i \in R$. Let $P_0 = \{5\}, \{3\}, \{3, 5\}$ when $(ii), (iii), (iv)$ holds, respectively. Then $\left(\frac{a_i}{p}\right) = 1$ for $p \in P_0$.

Assume that $7 \nmid d$ when $8|d, 15|d$. Let $\mathcal{P} = \{7\}$ if $8|d, 3|d, 5 \nmid d$; $\mathcal{P} = \{7, 11, 13, 17, 19\}$ if $4||d, 15|d$; $\mathcal{P} = \{11, 13, 17, 19\}$ if $8|d, 15|d$ and $\mathcal{P} = \{7, 11, 13\}$ in all other cases. Suppose that $p' \nmid d$ for some prime $p' \in \mathcal{P}$. Let r be given by the following table:

$(ii), (iii), 2\|\|d, 4\|\|d$	$(ii), (iii), 8\|d$	$(iv), 2\|\|d$	$(iv), 4\|\|d, 8\|d$
$\begin{cases} 8 & \text{for } k \le 941 \\ 9 & \text{for } k > 941 \end{cases}$	$\begin{cases} 10 & \text{for } k \le 941 \\ 11 & \text{for } k > 941 \end{cases}$	9	11

We get $\mathcal{B}_r \subseteq W_1$. For $s \in W_1'$, we get from (9.5.1) that $\nu(s) = \nu_o(s) \le G(k,s,\delta) := \min(f_0(k,s,\delta), G_1, G_2)$ where

$$(G_1, G_2) = \begin{cases} (f_1(k,s,3,2,\delta), \max_{p' \in \mathcal{P}} f_2(k,s,3,p',2,\delta)) & \text{when } (ii) \text{ holds, } 8 \nmid d \\ (f_1(k,s,5,1,\delta), \max_{p' \in \mathcal{P}} f_2(k,s,5,p',1,\delta)) & \text{when } (iii) \text{ holds, } 8 \nmid d \\ (f_1(k,s,3,1,3), \max_{p' \in \mathcal{P}} f_2(k,s,3,p',2,3)) & \text{when } (ii) \text{ holds, } 8|d \\ (f_1(k,s,5,1,3), \max_{p' \in \mathcal{P}} f_2(k,s,5,p',2,3)) & \text{when } (iii) \text{ holds, } 8|d \end{cases}$$

and when (iv) holds, $G_1 = G_2 = \max_{p' \in \mathcal{P}} f_1(k,s,p',1,\delta)$ if $2||d$ or $4||d$, $G_1 = G_2 = \max_{p' \in \mathcal{P}} f_2(k,s,7,p',1,3)$ if $8|d$. Therefore $\xi_r \le g' + \sum_{s \in W_1'}(G(k,s,\delta) - 1) =: \tilde{\xi_r}$. Now we check (11.1.2) contradicting (9.2.1). Thus $p'|d$ for each prime $p' \in \mathcal{P}$. Let r and g_1 be given by the following table:

Cases:	$(ii),(iii),2\|\|d$	$(ii),(iii),4\|\|d$	$(ii),8\|d$	$(iv),2\|\|d$	$(iv),8\|d$
(r,g_1)	$(12,8)$	$(12,4)$	$(15,16)$	$(13,4)$	$(17,4)$

Suppose that one of the above case hold. Then $\mathcal{B}_r \subseteq \{s \in \mathcal{S}(r) : s \equiv 1(\text{mod } 2^\delta), \left(\frac{s}{p'}\right) = 1, p' \in \mathcal{P} \cup \mathcal{P}_0\} = \{1\} \cup W^{''}$ with $|W^{''}| = g_1 - 1$ and $s \ge \frac{2000}{2^{3-\delta}}$ for $s \in W^{''}$. Therefore $\xi_r \le \nu(1) + g_1 - 1$. From (9.5.1), we get $\nu(1) \le G(k)$ where $G(k) = f_1(k,1,3,2,\delta)$ if (ii) holds; $f_1(k,1,5,2,\delta)$ if (iii) holds, $8 \nmid d$; $G(k) = f_0(k,1,1)$ if (iv) holds with $2||d$ and $G(k) = f_1(k,1,7,2,3)$ if (iv) holds with $8|d$. Therefore $\xi_r \le G(k) + g_1 - 1 =: \tilde{\xi_r}$ and we compute that (11.1.2) holds. This contradicts (9.2.1). Thus either $(A) : (iv)$ holds, $4||d$ or $(B) : (iii)$ holds, $8|d$. Assume that $p' \nmid d$ with $p' \in \mathcal{P}_1$ where $\mathcal{P}_1 = \{23, 29, 31, 37\}, \{11, 13, 17, 19\}$ when $(A), (B)$ holds, respectively. In the remaining part of this paragraph, by 'respectively", we mean "when $(A), (B)$ holds, respectively'. We take $r = 18, 11$, respectively. Then $\mathcal{B}_r \subseteq \{s \in \mathcal{S}(r) : s \equiv 1(\text{mod } 2^\delta), \left(\frac{s}{p'}\right) = 1, p' \in \mathcal{P} \cup \mathcal{P}_0\} \subseteq \{1, 1705\} \cup W^{''}$ with $|W^{''}| = g_1$ and $s \ge \frac{2000}{2^{3-\delta}}$ for $s \in W^{''}$ where $g_1 = 3, 14$, respectively. Hence $\xi_r \le \nu(1) + \nu(1705) + g_1 \le G(k) + 2 + g_1 =: \tilde{\xi_r}$ where $\nu(1) \le G(k) = \max_{p' \in \mathcal{P}_1} f_1(k,1,p',1,2), \max_{p' \in \mathcal{P}_1} f_2(k,1,5,p',1,3)$, respectively by (9.5.1). We check (11.1.2), contradicting (9.2.1). Thus $p'|d$ with $p' \le 37$ if (A) holds and $p'|d$ with $p' \le 19, p' \ne 5$ if (B) holds. Now we take $r = 22, 16$, respectively to get $\mathcal{B}_r \subseteq \{1\} \cup W^{''}$ with $|W^{''}| = g_2$ and $s \ge \frac{2000}{2^{3-\delta}}$ for $s \in W^{''}$ where $g_2 = 0, 3$, respectively. From (9.5.1), we get $\nu(1) \le G(k)$ with $G(k) = f_0(k,1,2), f_1(k,1,5,2,3)$, respectively. Hence $\xi_r \le G(k) + g_2 =: \tilde{\xi_r}$ and we compute that (11.1.2) holds. This contradicts (9.2.1).

Thus it remains to consider the case (iv) with $8|d$ and $7|d$. Then

$$a_i \equiv 1(\text{mod } 8) \text{ and } \left(\frac{a_i}{p}\right) = 1 \text{ for } p = 3, 5, 7 \tag{11.1.3}$$

whenever $a_i \in R$. Let $k < 263$. By taking $r = 12$, we find that $\mathcal{B}_r \subseteq \{s \in \mathcal{S}(r) : s \equiv 1(\text{mod } 8), \left(\frac{s}{p_j}\right) = 1, 2 \le j \le 4\} = \{1, 6409, 9361, 12121, 214489, 268801, 4756609, 59994649\}$. Then by Lemma 9.5.3, $\nu(1) \le \frac{k-1}{2}$ since $k \nmid d$ by our assumption. Further $\nu(6409) + \nu(268801) + \nu(4756609) + \nu(59994649) \le \left\lceil \frac{k}{13 \cdot 29} \right\rceil \le 1$, $\nu(9361) + \nu(214489) \le \left\lceil \frac{k}{11 \cdot 37} \right\rceil \le 1$ and $\nu(12121) \le 1$. Therefore $\xi_r \le \frac{k-1}{2} + 3 =: \tilde{\xi_r}$. We check (11.1.2) contradicting (9.2.1). Thus $k \ge 263$. By (11.1.3), we see that a_i is not a prime ≤ 89. Hence for $a_i \in R$ with $P(a_i) \le 89$, we have $\omega(a_i) \ge 2$. Further by (11.1.3), $a_i = p'q'$ with $11 \le p' \le 37$ and $41 \le q' \le 89$ is not possible. For integers P_1, P_2 with $P_1 < P_2$, let

$$\mathcal{I}(P_1, P_2) = \{i : p'q'|a_i, P_1 \le p' < q' \le P_2\}.$$

Then $|\mathcal{I}(P_1, P_2)| \le \sum_{P_1 \le p' < q' \le P_2} \left\lceil \frac{k}{p'q'} \right\rceil$. Suppose that $p_j \nmid d$ for some prime $j \in \{5, 6\}$. Then $\nu(1) \le G_0(k) := \max_{j=5,6} f_1(k,1,p_j,2,3)$ by (9.5.1). We take $r = 23$. For $P_0 \in \{11, 13\}$, let $A(P_0) = \{a_i : a_i = P_0 p'$ with $P_0 < p' \le 37$ or $a_i = P_0 p' q'$ with $P_0 < p' \le 37, 41 \le q' \le 83\}$. Then from (11.1.3), we get $A(11) \subseteq \{6721, 8569, 25201\}$ and $A(13) \subseteq \{17329, 17641, 27001\}$. Therefore we get from

$$\begin{aligned} I_r \subseteq &\{i : a_i = 1\} \cup \mathcal{I}(17, 37) \cup \mathcal{I}(41, 83) \cup \\ &\{i : a_i \in A(11) \cup A(13)\} \cup \{i : 11 \cdot 13p'|a_i, 17 \le p' \le 37\} \end{aligned}$$

that

$$\xi_r \le G_0(k) + \sum_{17 \le p' < q' \le 37} \left\lceil \frac{k}{p'q'} \right\rceil + \left\lceil \frac{k}{41 \cdot 43} \right\rceil + 54 + 3 + 3 + 6 =: \tilde{\xi_r}$$

since $p'q' > k$ for $41 \le p' < q' \le 83$ except when $p' = 41, q' = 43$. Now we compute that (11.1.2) holds contradicting (9.2.1). Thus $p_j|d$ for $j \le 6$. Assume that $p_j \nmid d$ for some j with $7 \le j \le 9$. Then $\nu(1) \le G_1(k) := \max_{7 \le j \le 9} f_1(k, 1, p_j, 1, 3)$ by (9.5.1). We take $r = 24$. Then $I_r \subseteq \{i : a_i = 1\} \cup \mathcal{I}(17, 37) \cup \mathcal{I}(41, 89)$. Therefore $\xi_r \le G_1(k) + \sum_{17 \le p' < q' \le 37} \lceil \frac{k}{p'q'} \rceil + \lceil \frac{k}{41 \cdot 43} \rceil + 65 =: \tilde{\xi_r}$ and we check (11.1.2). This contradicts (9.2.1). Thus $p_j|d$ for $j \le 9$. Suppose that $p_j \nmid d$ for some j with $10 \le j \le 14$. Then $\nu(1) \le G_2(k) := \max_{10 \le j \le 14} f_1(k, 1, p_j, 1, 3)$ by (9.5.1). We take $r = 21$. Then $\mathcal{B}_r \subseteq \{s \in \mathcal{S}(r) : s \equiv 1 (\text{mod } 8)$ and $\left(\frac{s}{p_i}\right) = 1, i \le 9\} = \{1, 241754041\}$ giving $\xi_r \le G_2(k) + 1 =: \tilde{\xi_r}$. Now we check (11.1.2) contradicting (9.2.1). Hence $p_j|d$ for $j \le 14$. Suppose that $p_j \nmid d$ for some j with $15 \le j \le 22$. Then $\nu(1) \le G_3(k) := \max_{15 \le j \le 22} f_1(k, 1, p_j, 1, 3)$ by (9.5.1). We take $r = 26$. Then $\mathcal{B}_r \subseteq \{1\}$ as above giving $\xi_r \le G_2(k) =: \tilde{\xi_r}$. We compute that (11.1.2) holds contradicting (9.2.1). Thus $p_j|d$ for $j \le 22$. Finally we take $r = 32$. Then $\mathcal{B}_r \subseteq \{1\}$ as above giving $\xi_r \le \nu(1) \le \frac{k-1}{2} =: \tilde{\xi_r}$ by Lemma 9.5.3. We check (11.1.2). This contradicts (9.2.1). □

LEMMA 11.1.2. *We have*

(11.1.4) $$k - |R| \ge g \text{ for } k \ge k_0(g)$$

where g and $k_0(g)$ are given by
(i)

g	9	14	17	29	33	61	65	129	256	2^s *with* $s \ge 9,\ s \in \mathbb{Z}$
$k_0(g)$	101	299	308	489	556	996	1057	2100	4252	$s2^{s+1}$

(ii) d even:

g	18	29	33	61	64	128	256	512	1024
$k_0(g)$	101	223	232	409	430	900	1895	4010	8500

(iii) $4||d$:

g	26	32	33	61	64	128	256	512	1024
$k_0(g)$	101	126	129	286	303	640	1345	2860	6100

(iv) $8|d$:

g	33	61	64	128	256	512	1024
$k_0(g)$	101	209	220	466	990	2110	4480

(v) $3|d$:

g	26	32	33	64	125	128	256	512
$k_0(g)$	101	126	129	351	720	735	1550	3300

(vi) $p|d$ with $p \in \{5, 7\}$:

g	33	64	128	256
$k_0(g)$	240	460	930	1940

Further we have $k_0(128) = 1200$ if $p|d$ with $p \le 19$ and $k_0(256) = 2870$ if $p|d$ with $p \le 47$.
(vii) Further $k_0(256) = 1115$ if $pq|d$ with $p \in \{5, 7, 11\}$; $k_0(256) = 1040$ if $2p|d$ with $p \in \{3, 5\}$; $k_0(512) = 1400$ if $105|d$; $k_0(512) = 1440$ if $30|d$ and $k_0(512) = 1480$ if $8p|d$ with $p \in \{3, 5\}$.

PROOF. (i) Let g be given as in (i). Assume that $k \geq k_0(g)$ and $k - |R| < g$. We shall arrive at a contradiction.

Let $g \neq 9$. From (9.4.9), we have $\prod_{a_i \in R} a_i \geq (1.6)^{|R|}(|R|)!$ whenever $|R| \geq 286$. We observe that (9.3.28) and (9.3.29) hold with $i_0 = 0, h_0 = 286$, $z_1 = 1.6, g_1 = g - 1$, $\mathfrak{m}$ =min(89, $\sqrt{k_0(g)}$), $\ell = 0, \mathfrak{n}_0 = 1, \mathfrak{n}_1 = 1$ and $\mathfrak{n}_2 = 2^{\frac{1}{6}}$ for $k \geq g_1 + 286$ and thus for $k \geq k_0(g)$.

Let $g = 2^s$ with $s \geq 9$. Then $\frac{g_1}{k} \leq \frac{2^s}{s2^{s+1}} \leq \frac{1}{18}$ and we get from (9.3.29)

$$2^s - 1 > \frac{c_1 k - c_2 \log k - c_3}{\log c_4 k} = \frac{c_1 k - c_3 + c_2 \log c_4}{\log c_4 k} - c_2 \tag{11.1.5}$$

where

$$c_1 = \log\left(\frac{1.6}{2.71851}\prod_{p\leq\mathfrak{m}} p^{\frac{2}{p^2-1}}\right) + \log(1 - \frac{1}{18}),\ c_2 = 1.5\pi(\mathfrak{m}) - 1,$$

$$c_3 = \log\left(2^{\frac{1}{6}}\prod_{p\leq\mathfrak{m}} p^{.5+\frac{2}{p^2-1}}\right) - \frac{1}{2}\log(1-\frac{1}{18}),\quad c_4 = \frac{1.6}{e}$$

Here we check that $c_1 k - c_2 \log k - c_3 > 0$ at $k = 9 \cdot 2^{10}$ and hence (11.1.5) is valid. Further we observe that the right hand side of (11.1.5) is an increasing function of k. Putting $k = k_0(g) = s2^{s+1}$, we get from (11.1.5) that

$$2^s\left\{\frac{2c_1 - \frac{c_3 - c_2\log c_4}{s2^s}}{\log 2 + \frac{\log(2c_4 s)}{s}} - \frac{c_2 - 1}{2^s} - 1\right\} < 0.$$

The expression inside the brackets is an increasing function of s and it is positive at $s = 9$. Hence (11.1.5) does not hold for all $k \geq k_0(g)$. Therefore $k - |R| \geq g = 2^s$ whenever $s \geq 9$ and $k \geq s2^{s+1}$.

Let $g \in \{14, 17, 29, 33, 61, 65, 129, 256\}$ and $k_1(g) = 299, 316, 500, 569, 1014, 1076, 2126, 4295$ according as $g = 14, 17, 29, 33, 61, 65, 129, 256$, respectively. We see that the right hand side of (9.3.29) is an increasing function of k and we check that it exceeds g_1 at $k = k_1(g)$. Therefore (9.3.29) is not possible for $k \geq k_1(g)$. Thus $g \neq 14$ and $k < k_1(g)$. For every k with $k_0(g) \leq k < k_1(g)$, we compute the right hand side of (9.3.28) and we find it greater than g_1. This is not possible.

Thus we may assume that $g = 9$ and $k < 299$. By taking $r = 4$ for $101 \leq k \leq 181$ and $r = 5$ for $181 < k < 299$ in (9.2.3) and (9.2.5), we get $k - |R| \geq k - F'(k, r) - 2^r \geq 9$ for $k \geq 101$ except when $103 \leq k \leq 120, k \neq 106$ where $k - |R| \geq k - F(k, r) - 2^r \geq k - F'(k, r) - 2^r = 8$. Let $103 \leq k \leq 120, k \neq 106$. We may assume that $k - |R| = 8$ and hence $F(k, r) = F'(k, r)$. Thus for each prime $11 \leq p \leq k$, there are exactly σ_p number of i's for which $p|a_i$ and for any i, $pq \nmid a_i$ whenever $11 \leq q \leq k, q \neq p$. Now we get a contradiction by considering the i's for which a_i's are divisible by primes $17, 101; 103, 17; 13, 103; 53, 13; 107, 53; 11, 109; 37, 11; 19, 113; 23, 19; 29, 23; 13, 29; 59, 13; 17, 59$ when $k = 103, 104, 105, 107, 108, 111, 112, 115, 116, 117, 118, 119, 120$, respectively; $107, 53, 13, 103, 17$ when $k = 109$, $109, 107, 53$ when $k = 110$; $37, 11, 109, 107$ when $k = 113$ and $113, 37, 11$ when $k = 114$. For instance let $k = 113$. Then $37|a_i$ for $i \in \{0, 37, 74, 111\}$ or $i \in \{1, 38, 75, 112\}$. We consider the first case and the other case follows similarly. Then $11|a_i$ for $i \in \{2 + 11j : 0 \leq j \leq 10\}$ and $109|a_i$ for $i \in \{1, 110\}$. Now $\sigma_{107} = 2$ implies that $107|a_i a_{i+107}$ for $i \in \{j : 0 \leq j \leq 5\}$, a contradiction. The other cases are excluded similarly.

(ii) Let d be even and g be given as in (ii). Assume that $k \geq k_0(g)$ and $k - |R| < g$. From (9.4.10), we have $\prod_{a_i \in R} a_i \geq (2.4)^{|R|}(|R|)!$ whenever $|R| \geq 200$. By taking $i_0 = 0, h_0 = 200$, $\mathfrak{m} = \sqrt{k_0(g)}$, $z_1 = 2.4, \ell = 1$, $\mathfrak{n}_0 = 2^{\frac{1}{3}}, \mathfrak{n}_1 = 2^{\frac{1}{6}}$ and $\mathfrak{n}_2 = 1$, we observe that (9.3.28) and (9.3.29) are valid for $k \geq g - 1 + 200$. Let $g \in \{33, 61, 64, 128, 256, 512, 1024\}$. Thus (9.3.28) and (9.3.29) are valid for $k \geq k_0(g)$. Let $k_1(g) = 232, 414, 435, 904, 1907, 4024, 8521$ according as $g = 33, 61, 64, 128, 256, 512, 1024$, respectively. We see that (9.3.29) is not possible for $k \geq k_1(g)$. Therefore $g \neq 33$ and $k < k_1(g)$. For every k with $k_0(g) \leq k < k_1(g)$, we check that (9.3.28) is contradicted. Therefore $g \in \{18, 29\}$ and we may assume that $k < 232$. We take $r = 5$ for $101 \leq k < 200$ and $r = 6$ for $200 \leq k < 232$. From (9.2.10) and (9.2.6), we get $k - |R| \geq k - F'(k, r) - 2^{r-1}$. We compute that $k - F'(k, r) - 2^{r-1} \geq 18, 29$ for $k \geq 101, 217$, respectively. Hence the assertion (ii) follows.

$(iii), (iv)$ Let g be given as in $(iii), (iv)$. Suppose that $k \geq k_0(g)$ and $k - |R| < g$. We have $\prod_{a_i \in R} a_i \geq (2^\delta)^{|R|-1}(|R|-1)!$ since $a_i \equiv n(\text{mod } 2^\delta)$. We take $z_1 = 4$ if $4||d$ and $z_1 = 8$ if $8|d$. We observe that (9.3.28) and (9.3.29) are valid for $k \geq k_0(g)$ with $i_0 = 1, h_0 = 1$, $\mathfrak{m} = \sqrt{k_0(g)}$, $z_1 = 2, \ell = 1$, $\mathfrak{n}_0 = 2^{\frac{1}{3}}, \mathfrak{n}_1 = 2^{\frac{1}{6}}$ and $\mathfrak{n}_2 = 1$.

Let $4||d$ and $g \in \{61, 64, 128, 256, 512, 1024\}$. Let $k_1(g) = 288, 306, 640, 1350, 2870, 6100$ according as $g = 61, 64, 128, 256, 512, 1024$, respectively. We see that (9.3.29) is not possible for $k \geq k_1(g)$. Therefore $g \neq 128, 1024$ and $k < k_1(g)$. For every k with $k_0(g) \leq k < k_1(g)$, we check that (9.3.28) is contradicted.

Let $8|d$ and $g \in \{61, 64, 128, 256, 512, 1024\}$. Let $k_1(g) = 210, 221, 468, 994, 2111, 4485$ according as $g = 61, 64, 128, 256, 512, 1024$, respectively. We see that (9.3.29) is not possible for $k \geq k_1(g)$. Therefore $k < k_1(g)$. For every k with $k_0(g) \leq k < k_1(g)$, we check that (9.3.28) is contradicted.

Thus we may assume that $g \in \{26, 32, 33\}, k < 286$ if $4||d$ and $g = 33, k < 209$ if $8|d$. By taking $r = 6$ for $101 \leq k < 286$, we get from (9.2.10) and (9.2.6) that $k - |R| \geq k - F'(k,r) - 2^{r-\delta} \geq g$ for $k \geq k_0(g)$. Hence the assertions (iii) and (iv) follows.

(v) Let $3|d$. Suppose that $k \geq k_0(g)$ and $k - |R| < g$. We have $\prod_{a_i \in R} a_i \geq 3^{|R|-1}(|R|-1)!$ since $a_i \equiv n(\text{mod } 3)$. We observe that (9.3.28) and (9.3.29) are valid with $i_0 = 1, h_0 = 1, \mathfrak{m} = \sqrt{k_0(g)}$, $z_1 = 3, \ell = 1$, $\mathfrak{n}_0 = 3^{\frac{1}{4}}$, $\mathfrak{n}_1 = 3^{\frac{1}{4}}$ and $\mathfrak{n}_2 = 2^{\frac{1}{6}}$. Let $g \in \{64, 125, 128, 256, 512\}$ and $k_1(g) = 354, 720, 737, 1556, 3300$ according as $g = 64, 125, 128, 256, 512$, respectively. We see that (9.3.29) is not possible for $k \geq k_1(g)$. Therefore $g \neq 125, 512$ and $k < k_1(g)$. For every k with $k_0(g) \leq k < k_1(g)$, we check that (9.3.28) is contradicted.

Thus it remains to consider $g \in \{26, 32, 33\}$ and $k < 351$. We take $r = 6$ for $101 \leq k < 351$. We get from (9.2.10) and (9.2.14) with $p = 3$ that $k - |R| \geq k - F'(k,r) - 2^{r-2} \geq g$ for $k \geq k_0(g)$.

(vi) Suppose $g \in \{33, 64, 128, 256\}, k \geq k_0(g)$ and $k - |R| < g$. By (ii) and (v), we may assume that $2 \nmid d$ and $3 \nmid d$. We observe that $\prod_{a_i \in R} a_i \geq (\frac{2p}{p-1})^{|R|-\frac{p-1}{2}}(|R| - \frac{p-1}{2})!$ since the number of quadratic residues or quadratic non-residues mod p is $\frac{p-1}{2}$. Let $p|d$ with $p \leq p'$. Then $(\frac{2p}{p-1})^{|R|-\frac{p-1}{2}}(|R| - \frac{p-1}{2})! \geq (\frac{2p'}{p'-1})^{|R|-\frac{p'-1}{2}}(|R| - \frac{p'-1}{2})$. We take $p' = 7, 19$ and 47 in the first, second and third case, respectively. Then (9.3.28) and (9.3.29) are valid with $z_1 = \frac{2p'}{p'-1}, i_0 = h_0 = \frac{p'-1}{2}$, $\mathfrak{m} = \sqrt{k_0(g)}, \ell = 1$, $\mathfrak{n}_0 = p'^{\frac{1}{p'+1}}$, $\mathfrak{n}_1 = 5^{\frac{1}{3}}$ and $\mathfrak{n}_2 = 2^{\frac{1}{6}}$. We find that (9.3.29) is not possible for $k \geq k_0(g) + 24$ and (9.3.28) is not possible for each k with $k_0(g) \leq k < k_0(g) + 24$. This is a contradiction.

(vii) Let $(z_1, i_0, \ell', \mathfrak{n}'_0, \mathfrak{n}'_1)$ be given by

	$pq\|d,\ p, q \in \{5, 7, 11\}$	$2^\delta p\|d,\ \delta \in \{1, 3\}, p \in \{3, 5\}$	$105\|d$	$30\|d$
(z_1, i_0)	$(\frac{77}{15}, 15)$	$(2^{\delta-1}5, 2)$	$(\frac{35}{2}, 6)$	$(15, 2)$
ℓ'	2	2	3	3
$\mathfrak{n}'_0$	$z_2(7)z_2(11)$	$z_2(2)z_2(5)$	$z_2(3)z_2(5)z_2(7)$	$z_2(2)z_2(3)z_2(5)$
$\mathfrak{n}'_1$	$z_3(5)z_3(7)$	$z_3(2)z_3(3)$	$z_3(3)z_3(5)z_3(7)$	$z_3(2)z_3(3)z_3(5)$
$\mathfrak{n}'_2$	$2^{\frac{1}{6}}$	1	$2^{\frac{1}{6}}$	1

where $z_2(p) = p^{\frac{1}{p+1}}, z_3(p) = p^{\frac{p-1}{2(p+1)}}$. We observe that $\prod_{a_i \in R} a_i \geq z_1^{|R|-i_0}(|R|-i_0)!$ with (z_1, i_0) given above. Suppose $g \in \{256, 512\}, k \geq k_0(g)$ and $k - |R| < g$. We see that (9.3.28) and (9.3.29) are valid for $k \geq k_0(g)$ with $h_0 = i_0$, $\mathfrak{m} = \sqrt{k_0(g)}$, $\ell = \ell'$, $\mathfrak{n}_0 = \mathfrak{n}'_0, \mathfrak{n}_1 = \mathfrak{n}'_1$ and $\mathfrak{n}_2 = \mathfrak{n}'_2$. We find that (9.3.29) is not possible for $k \geq k_0(g) + 2$ and (9.3.28) is not possible for each k with $k_0(g) \leq k < k_0(g) + 2$. This is a contradiction. □

Lemma 11.1.3. *We have*

$$|T_1| > \alpha k \text{ for } k \geq K_\alpha \tag{11.1.6}$$

where α and K_α are given by

α	.3	.35	.4	.42
K_α	101	203	710	1639

Proof. Let $k \geq K_\alpha$. Thus $k \geq 101$. From Theorem 1.5.1, we have $n + (k-1)d > 4k^2$. We see from (9.4.1) that

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

Therefore $n + (k-1)d > (\frac{k}{2}\log\frac{k}{2})^2$ by Lemma 3.1.2 (v).

For $0 < \beta < 1$, let

$$n + (k-1)d > (\beta k \log \beta k)^2. \tag{11.1.7}$$

We may assume that $\beta \geq \frac{1}{2}$. Put $X_\beta = X_\beta(k) = \beta \log(\beta k)$. Then $\log(n+(k-1)d) > 2\log X_\beta + 2\log k$. From (9.4.1), we see that

$$\begin{aligned} |T_1| + \pi_d(k) >& k - 1 - \frac{(k-1)\log k}{2\log X_\beta + 2\log k} = \frac{k}{2}\left(1 - \frac{1}{k}\right)\left(1 + \frac{\log X_\beta}{\log X_\beta + \log k}\right) \\ =& \frac{k}{2}\left(1 - \frac{1}{k}\right)\left(1 + \frac{1}{1 + \frac{\log k}{\log X_\beta}}\right) =: g_\beta(k)k =: g_\beta k. \end{aligned} \tag{11.1.8}$$

By using $\pi_d(k) \leq \pi(k)$ and Lemma 3.1.2 (i), we get from (11.1.8) that

$$|T_1| > g_\beta k - \frac{k}{\log k}\left(1 + \frac{1.2762}{\log k}\right). \tag{11.1.9}$$

Let $\beta = \frac{1}{2}$. We observe that

$$\frac{14}{13}\log k - \left(1 + \frac{\log k}{\log X_\beta}\right)\left(1 + \frac{1.2762}{\log k}\right) = \left(\frac{14}{13} - \frac{1}{\log X_\beta}\right)\log k - \left(\frac{1.2762}{\log k} + \frac{1.2762}{\log X_\beta}\right) - 1$$

is an increasing function of k and it is positive at $k = 2500$. Therefore

$$\frac{1}{1 + \frac{\log k}{\log X_\beta}} > \frac{13}{14}\frac{1}{\log k}\left(1 + \frac{1.2762}{\log k}\right) \text{ for } k \geq 2500$$

which, together with (11.1.9) and (11.1.8), implies

$$\frac{|T_1|}{k} > \frac{1}{2} - \frac{1}{2k} - \frac{1}{28\log k}\left(1 + \frac{1.2762}{\log k}\right)\left(15 + \frac{13}{k}\right) > .42 \text{ for } k \geq 2500$$

since the middle expression is an increasing function of k. Thus we may suppose that $k < 2500$. From (11.1.8), we get $|T_1| + \pi_d(k) > g_{\frac{1}{2}}k =: \beta_1 k$. Then (11.1.7) is valid with β replaced by β_1 and we get from (11.1.8) that $|T_1| + \pi_d(k) > g_{\beta_1}k =: \beta_2 k$. We iterate this process with β replaced by β_2 to get $g_{\beta_2} =: \beta_3$ and further with β_3 to get $|T_1| + \pi_d(k) > g_{\beta_3}k =: \beta_4 k$. Finally we see that $|T_1| > \beta_4 k - \pi(k) \geq \alpha k$ for $k \geq K_\alpha$. □

11.2. Further Lemmas

We observe that (9.3.24) is satisfied when $k \geq 11$ by Theorem 1.5.1. We shall use it without reference in this section.

Lemma 11.2.1. *Let d be odd and p, q be primes dividing d. Let $\omega(d) \leq 4$ and $k \leq 821$. Assume that $g_{p,q}(r) \leq 2^{r-\omega(d)}$ for $r = 5, 6$. Then* (2.1.1) *with $k \geq 101$ has no solution.*

Proof. Suppose equation (2.1.1) has a solution. Let $r = 5$ if $101 \leq k < 257$ and $r = 6$ if $257 \leq k \leq 821$. From (9.2.9), $\nu(a_i) \leq 2^{\omega(d)}$ and (9.2.1), we get $k - F'(k,r) \leq \xi_r \leq 2^{\omega(d)}g_{p,q} \leq 2^r$. We find $k - F'(k,r) > 2^r$ by computation. This is a contradiction. □

Lemma 11.2.2. *Equation* (2.1.1) *with $k \geq 101$ and $\omega(d) \leq 4$ is not possible.*

Proof. We may assume that k is prime by Lemma 9.1.1. Let d be even. For $k-|R| \geq \mathfrak{h}(5) = 4(2^{\omega(d)-\theta}-1)+1$, we get from Corollary 9.3.10 with $z_0 = 5$ that $n+(k-1)d < \frac{3}{Q}k^3$ with $Q = 32$ if $2||d$ and 16 if $4|d$. Let $\omega(d) \leq 3$. Since $k-|R| \geq \mathfrak{h}(5)$ by Lemma 11.1.2 $(ii), (iii), (iv)$ and $|S_1| \geq \frac{|T_1|}{2^{\omega(d)-\theta}} \geq \frac{.3k}{2^{3-\theta}}$ by Lemma 11.1.3, we get $\frac{3}{Q}k^3 > n+(k-1)d > 2^\delta(\frac{.3k}{2^{3-\theta}}-1)k^2$, a contradiction. Thus $\omega(d) = 4$. Let $k \geq 710$. Then $k-|R| \geq \mathfrak{h}(5)$ by Lemma 11.1.2 and $|S_1| \geq \frac{|T_1|}{2^{\omega(d)-\theta}} \geq \frac{.4k}{2^{4-\theta}}$ by Lemma 11.1.3. Hence we get $\frac{3}{Q} > n+(k-1)d > 2^\delta(\frac{.4k}{2^{4-\theta}}-1)k^2$, a contradiction again. Therefore $k < 710$. By Lemma 11.1.2, we get $k-|R| \geq \mathfrak{h}(3)$ implying $d < \frac{3}{16}k^2$ if $2||d$ and $d < \frac{3}{4}k^2$ if $4|d$ by Corollary 9.3.10 with $z_0 = 3$. However $d \geq 2^\delta \cdot 53 \cdot 59 \cdot 61$ by Lemma 11.1.1 (c). This is a contradiction.

Thus d is odd. Suppose $|S_1| \leq |T_1| - \mathfrak{h}(3)$. By Lemma 9.3.12, we have

$$d < \frac{\rho}{48}k^2, \ n+(k-1)d < \frac{\rho}{48}k^3. \tag{11.2.1}$$

Let $k \geq 710$. Since $\nu(a_i) \leq 2^{\omega(d)}$, we derive from Lemma 11.1.3 that $|S_1| \geq \frac{|T_1|}{2^{\omega(d)}} > \frac{.4k}{16} = .025k$. Therefore $\max\limits_{A_i \in S_1} A_i > \rho(.025k-1)$ giving $n+(k-1)d > \rho(.025k-1)k^2$ which contradicts (11.2.1). Thus $k < 710$. We see from Lemma 11.1.3 that $|T_1| > .3k$. For $\omega(d) \leq 3$, we have $\max\limits_{A_i \in S_1} A_i > \rho(\frac{.3k}{8}-1)$ giving $n+(k-1)d > \rho(\frac{.3k}{8}-1)k^2$ which contradicts (11.2.1). Let $\omega(d) = 4$. By Lemma 11.1.1 (a), we see that $d \geq$min$(3 \cdot 53 \cdot 59 \cdot 61, 23 \cdot 29 \cdot 31 \cdot 37) > \frac{3}{48}k^2$ contradicting (11.2.1).

Hence $|S_1| \geq |T_1| - \mathfrak{h}(3) + 1$. Therefore

$$n+(k-1)d \geq \rho(|T_1| - \mathfrak{h}(3))k^2. \tag{11.2.2}$$

Let $k-|R| \geq \mathfrak{h}(5)$. By Corollary 9.3.10 with $z_0 = 5$, we get $n+(k-1)d < \frac{3}{16}k^3$ which, together with $|T_1| \geq .3k$ by Lemma 11.1.3, contradicts (11.2.2) when $\omega(d) \leq 2$. Further $k \leq 133, 275$ when $\omega(d) = 3, 4$, respectively. Thus either

$$k - |R| < \mathfrak{h}(5) \tag{11.2.3}$$

or

$$\omega(d) > 2; \ k \leq 131 \text{ if } \omega(d) = 3; \ k \leq 271 \text{ if } \omega(d) = 4. \tag{11.2.4}$$

We now apply Lemma 11.1.2 (i) to get $\omega(d) \geq 2$ and $k \leq 293, 487, 991$ for $\omega(d) = 2, 3, 4$, respectively.

Let $3|d$. Then we have from Lemma 11.1.2 (v) that $\omega(d) > 2$ and $k \leq 131, 350$ when $\omega(d) = 3, 4$, respectively. By Lemma 11.1.1, we get $\mathfrak{p}_2 \geq 53$ and hence $53 \leq \mathfrak{p}_2 \leq \left(\frac{d}{3}\right)^{\frac{1}{\omega(d)-1}}$. By Corollary 9.3.10 with $z_0 = 3$ if $\omega(d) = 3$, $z_0 = 2$ if $\omega(d) = 4$ and Lemma 11.1.2 (v), we get $d < \frac{3}{4}k^2$ if $\omega(d) = 3$ and $< 3k^2$ if $\omega(d) = 4$. Therefore $53 \leq \mathfrak{p}_2 < \frac{k}{2} < 67$ if $\omega(d) = 3$ and $53 \leq \mathfrak{p}_2 < k^{\frac{2}{3}} \leq 350^{\frac{2}{3}} < 53$ if $\omega(d) = 4$. Therefore $\omega(d) = 3$ and $53 \leq \mathfrak{p}_2 \leq 61$. Now we get a contradiction from Lemma 11.2.1 with $(p, q) = (3, \mathfrak{p}_2)$ and (9.2.15).

Thus we may assume that $3 \nmid d$. Therefore $k \leq 293, 487, 991$ for $\omega(d) = 2, 3, 4$, respectively, as stated above. Let $\omega(d) = 4$ and $k < 308$. From $k - |R| \geq 9$ by Lemma 11.1.2 (i) and by Corollary 9.3.11, there exists a partition (d_1, d_2) of d such that $\max(d_1, d_2) < (k-1)^2$. Thus $\mathfrak{p}_1\mathfrak{p}_2 \leq \max(d_1, d_2) < (k-1)^2$ giving $\mathfrak{p}_1 < k-1$. By taking $r = 5$ for $101 \leq k < 251$, $r = 6$ for $251 \leq k < 308$, we get from (9.2.10) and $g_{\mathfrak{p}_1} \leq 2^{r-1}$ by (9.2.14) with $p = \mathfrak{p}_1$ that $k - |R| \geq k - F'(k, r) - 2^{r-1} \geq 16$. Now we return to $\omega(d) = 2, 3, 4$. By Lemma 11.1.2 (i), we get $k - |R| \geq 2^{\omega(d)}$. Then we see from Corollary 9.3.10 with $z_0 = 2$ that there is a partition (d_1, d_2) of d with $d_1 < k-1, d_2 < 4(k-1)$. Thus $\mathfrak{p}_1 < k$. We take $r = 5$ for $101 \leq k < 211$ and $r = 6$ for $211 \leq k < 556$ for the next computation and we use Lemma 11.1.2 (i) for $k \geq 556$. From (9.2.10) with $p = q = \mathfrak{p}_1$ and (9.2.14) with $p = \mathfrak{p}_1$, and since $\sum_{p|d, p>p_r} \sigma_p - g_{\mathfrak{p}_1} \geq 2 - 2^{r-1}$ if $\mathfrak{p}_1 > p_r$ and $\geq -2^{r-2}$ if $\mathfrak{p}_1 \leq p_r$, we get

$$k - |R| \geq k - F'(k, r) + 2 - 2^{r-1} \geq \begin{cases} 20 & \text{for } k \geq 101 \\ 29 & \text{for } k \geq 211 \\ 33 & \text{for } k \geq 251. \end{cases} \tag{11.2.5}$$

Therefore we get from (11.2.3), (11.2.4) that $\omega(d) > 2$ and $k \leq 199,991$ when $\omega(d) = 3, 4$, respectively.

Let $\omega(d) = 3$. By Corollary 9.3.10 with $z_0 = 3$, there is a partition (d_1, d_2) with $d_1 < \frac{k-1}{2}$ and $d_2 < 2(k-1)$. Thus $\mathfrak{p}_1\mathfrak{p}_2 \leq$max$(d_1, d_2) < 2(k-1)$ giving $\mathfrak{p}_1 < \sqrt{2(k-1)} \leq \sqrt{2 \cdot 198}$ and hence $p_1 \leq 19$. Further the possibility $p_1 = 19$ is excluded since $19 \cdot 23 > 2(k-1)$. Also $\mathfrak{p}_2 \leq 79, 53, 31, 29, 23$ for $\mathfrak{p}_1 = 5, 7, 11, 13, 17$, respectively. Now we apply Lemma 11.1.1 (a) to derive that either $\mathfrak{p}_1 = 5, 53 \leq \mathfrak{p}_2 \leq 79$ or $\mathfrak{p}_1 = 7, \mathfrak{p}_2 = 53$. Further from $5 \cdot 53 < 2(k-1)$, we get $k \geq 134$. Thus $k - |R| \leq 28$ by (11.2.3) and (11.2.4). Now we take $r = 6$ for $134 \leq k \leq 199$ in the next computation. We get from (9.2.10) and (9.2.15) with $(p, q) = (\mathfrak{p}_1, \mathfrak{p}_2)$ that $k - |R| \geq k - F'(k, r) - 2^{r-2} \geq 29$. This is a contradiction.

Let $\omega(d) = 4$. By Lemma 11.1.1 $(a), (b)$, we get $d \geq$min$(5{\cdot}53{\cdot}59{\cdot}61, 23{\cdot}47{\cdot}53{\cdot}59, 31{\cdot}41{\cdot}47{\cdot}53) = 953735$. Further by Corollary 9.3.10 with $z_0 = 2$ if $k < 251$, $z_0 = 3$ if $k \geq 251$ and (11.2.5), we obtain $d < 3k^2$ if $k < 251$ and $d < \frac{3}{4}k^2$ for $k \geq 251$. This is a contradiction since $k \leq 991$. □

Lemma 11.2.3. *Assume* (2.1.1) *with* $\omega(d) \geq 12$. *Suppose that*

$$d < \frac{3}{16}k^2, n + (k-1)d < \frac{3}{16}k^3. \tag{11.2.6}$$

Then $k < \omega(d)4^{\omega(d)}$.

Proof. Assume that $k \geq \omega(d)4^{\omega(d)}$. Then from $40 \cdot \left(\frac{3}{16}\right)^{\frac{2}{11}} < (12)^{\frac{7}{11}} 2^{\frac{36}{11}}$ and $\omega(d) \geq 12$, we get $\left(\frac{3k^2}{16}\right)^{\frac{2}{11}} \leq \frac{k}{40 \cdot 2^{\omega(d)}}$. This together with $\mathfrak{q}_1\mathfrak{q}_2 \leq \left(\frac{d}{2^{\delta\theta}}\right)^{\frac{2}{\omega(d)-\theta}} < \left(\frac{3k^2}{16}\right)^{\frac{2}{11}}$ by (9.1.10) and (11.2.6) gives $\mathfrak{q}_1\mathfrak{q}_2 < \frac{k}{40 \cdot 2^{\omega(d)}}$. Hence we derive from Corollary 9.3.7 (ii) with $d' = \mathfrak{q}_1\mathfrak{q}_2$ that

$$\nu(A_i) \leq 2^{\omega(d)-2-\theta} \text{ whenever } A_i \geq \frac{k}{40 \cdot 2^{\omega(d)}}. \tag{11.2.7}$$

Let

$$T^{(1)} = \{i \in T_1 : A_i > \frac{2^\delta \rho k}{6 \cdot 2^{\omega(d)}}\},\ T^{(2)} = T_1 \setminus T^{(1)} \tag{11.2.8}$$

and

$$S^{(1)} = \{A_i : i \in T^{(1)}\},\ S^{(2)} = \{A_i : i \in T^{(2)}\}. \tag{11.2.9}$$

Then considering residue classes modulo $2^\delta\rho$, we derive that

$$\frac{2^\delta \rho k}{6 \cdot 2^{\omega(d)}} \geq \max_{A_i \in S^{(2)}} A_i \geq 2^\delta \rho(|S^{(2)}| - 1) + 1$$

so that $|S^{(2)}| \leq \frac{k}{6 \cdot 2^{\omega(d)}} + 1 \leq \frac{k}{6 \cdot 2^{\omega(d)}} + 1$. We have from (11.2.8), (11.2.9) and (11.2.7) together with $\nu(A_i) \leq 2^{\omega(d)}$ by Corollary 9.3.7 (ii) that

$$\begin{aligned}|T^{(2)}| &\leq \frac{k}{40 \cdot 2^{\omega(d)}}2^{\omega(d)} + \left(\frac{k}{6 \cdot 2^{\omega(d)}} - \frac{k}{40 \cdot 2^{\omega(d)}} + 1\right)2^{\omega(d)-2} \\ &\leq \frac{k}{40} + \frac{1}{4}\left(\frac{k}{6} - \frac{k}{40}\right) + 2^{\omega(d)-2} \leq \frac{k}{24} + \frac{3k}{160} + \frac{k}{480} = \frac{k}{16}\end{aligned}$$

since $k \geq \omega(d)4^{\omega(d)}$ and $\omega(d) \geq 12$. By Lemma 11.1.3 and $k > 1639$, we have

$$|T^{(1)}| > |T_1| - |T^{(2)}| \geq .42k - \frac{k}{16} = .3575k.$$

Let $\mathfrak{C}$, $\mathfrak{C}_\mu$ be as in Lemma 9.4.7 with $c = 2$. Then $.3575k < |T^{(1)}| = |S^{(1)}| + \sum_{\mu \geq 2}(\mu - 1)|\mathfrak{C}_\mu| \leq |S^{(1)}| + \mathfrak{C} \leq |S^{(1)}| + \frac{3\log 2}{16}\omega(d)4^{\omega(d)}$ by Lemma 9.4.7. Now we use $\frac{3\log 2}{16} < \frac{1}{7.6}$ to get $.3575k < |S^{(1)}| + \frac{k}{7.6}$ implying $|S^{(1)}| > 0.2259k$. Therefore $n + (k-1)d \geq (\max_{A_i \in S^{(1)}} A_i)k^2 \geq 0.2259k^3$ contradicting (11.2.6). □

Lemma 11.2.4. *Assume* (2.1.1) *with* $\omega(d) \geq 5$. *Then there is no non-degenerate double pair.*

Proof. Assume (2.1.1) with $\omega(d) \geq 5$. Further we suppose that there exists a non-degenerate double pair. Then we derive from Lemma 9.3.4 with $z_0 = 2$ that

$$d < \mathcal{X}_0 k^2, \ n + (k-1)d < \mathcal{X}_0 k^3 \tag{11.2.10}$$

where

$$\mathcal{X}_0 = 3, \frac{3}{2}, 12, 6 \text{ if } 2 \nmid d, 2||d, 4||d, 8|d, \text{ respectively.} \tag{11.2.11}$$

This with $d \geq 2^\delta \prod_{i=2}^{\omega(d)+1-\delta'} p_i$ implies $k^2 > \frac{1}{6}\prod_{i=1}^{\omega(d)} p_i$. Therefore we get from Lemmas 3.1.1 (v) and 3.1.3 that

$$\log(\frac{k}{\omega(d)2^{\omega(d)}}) \geq \omega(d) \left\{ \frac{\log\omega(d) + \log\log\omega(d) - 1.076868}{2} - \log 2 - \frac{\log\omega(d)}{\omega(d)} \right\} - \frac{\log 6}{2}.$$

The right side of the above inequality is an increasing function of $\omega(d)$ and hence $k > 9\omega(d)2^{\omega(d)}$ for $\omega(d) \geq 12$. We find from $\mathcal{X}_0 k^2 > d \geq 2^\delta \prod_{i=2}^{\omega(d)+1-\delta'} p_i$ that $k > 3.2\omega(d)2^{\omega(d)}$ if $\omega(d) = 10, 11$. Further $k > 2.97\omega(d)2^{\omega(d)}$ if $\omega(d) = 8, 9$ when d is odd. Also $k > 2542, 12195$ when $\omega(d) = 8, 9$, respectively if $2||d$ or $8|d$ and $k > 1271, 6097$ when $\omega(d) = 8, 9$, respectively if $4||d$.

Suppose $k < 1733$. Then $\omega(d) \leq 8$ if $4||d$ and $\omega(d) < 8$ otherwise. By Lemma 11.1.1 (a), (c), we get $d \geq$min$(3 \cdot 53 \cdot 59 \cdot 61 \cdot 67, 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41)$ if d is odd and $d \geq 2^\delta \cdot 53 \cdot 59 \cdot 61 \cdot 67$ if d is even. This is not possible since $d < \mathcal{X}_0 k^2$. Hence $k \geq 1733$.

Let d be even and $\omega(d) = 8, 9$. Since $k \geq 1733$, we get $k - |R| \geq \mathfrak{h}(3)$ by Lemma 11.1.2 $(ii), (iii), (iv)$ implying $d < \frac{3}{16}k^2, \frac{3}{4}k^2$ if $2||d$, $4|d$, respectively, by Corollary 9.3.10 with $z_0 = 3$. Therefore $k \geq 2.48\omega(d)2^{\omega(d)}$ if $4||d$ and $k \geq 3.2\omega(d)2^{\omega(d)}$ otherwise.

Therefore for $\omega(d) \geq 8$, we have

$$k \geq \begin{cases} 2.48\omega(d)2^{\omega(d)} & \text{if } 4||d \\ 2.97\omega(d)2^{\omega(d)} & \text{if } d \text{ is odd, } \omega(d) = 8, 9 \\ 3.2\omega(d)2^{\omega(d)} & \text{otherwise} \end{cases} \tag{11.2.12}$$

Suppose that $|S_1| \leq |T_1| - \mathfrak{h}(3)$ if d is odd and $|S_1| \leq |T_1| - \mathfrak{h}(5)$ if d is even. We put

$$\mathcal{X} := \begin{cases} \frac{\rho}{48} & \text{if } \mathrm{ord}_2(d) \leq 1 \\ \frac{1}{12} & \text{if } \mathrm{ord}_2(d) \geq 2, 3 \nmid d \\ \frac{3}{16} & \text{if } \mathrm{ord}_2(d) \geq 2, 3|d. \end{cases}$$

Then

$$d < \mathcal{X}k^2, n + (k-1)d < \mathcal{X}k^3 \tag{11.2.13}$$

by Lemma 9.3.12. Therefore $k < \omega(d)4^{\omega(d)}$ for $\omega(d) \geq 12$ by Lemma 11.2.3.

Let $\omega(d) \geq 19$. Then

$$\left(2^\delta \prod_{i=2}^{9} p_i\right) (29)^{\omega(d)-8-\delta'} \leq d < \mathcal{X}k^2 < W := \begin{cases} \frac{3}{48}\omega(d)^2(16)^{\omega(d)} & \text{if } \mathrm{ord}_2(d) \leq 1 \\ \frac{3}{16}\omega(d)^2(16)^{\omega(d)} & \text{if } \mathrm{ord}_2(d) \geq 2. \end{cases}$$

Therefore

$$\frac{29}{16} < \left(\left(64 \prod_{i=3}^{9} p_i \right)^{-1} 29^9 \omega(d)^2 \right)^{\frac{1}{\omega(d)}}.$$

We see that the right hand side of the above inequality is a non-increasing function of $\omega(d)$ and the inequality does not hold at $\omega(d) = 26$. Thus $\omega(d) \leq 25$. Further we get a contradiction from $2^\delta \prod_{i=2}^{\omega(d)+1-\delta'} p_i \leq d < W$ since $\omega(d) \geq 19$.

Thus $\omega(d) \le 18$. We get from (9.1.10) and $d < \mathcal{X}k^2$ that

$$\mathfrak{q}_1 \cdots \mathfrak{q}_h < \mathcal{X}_1^h := \begin{cases} \left(\frac{\rho}{48}\right)^{\frac{h}{\omega(d)}} k^{\frac{2h}{\omega(d)}} & \text{if } d \text{ is odd} \\ \left(\frac{\rho}{96}\right)^{\frac{h}{\omega(d)-1}} k^{\frac{2h}{\omega(d)-1}} & \text{if } 2||d \\ \left(\frac{1}{12\cdot 4^\theta}\right)^{\frac{h}{\omega(d)-\theta}} k^{\frac{2h}{\omega(d)-\theta}} & \text{if } 4|d, 3\nmid d \\ \left(\frac{3}{16\cdot 4^\theta}\right)^{\frac{h}{\omega(d)-\theta}} k^{\frac{2h}{\omega(d)-\theta}} & \text{if } 4|d, 3|d \end{cases}$$

for $1 \le h \le \omega(d) - \theta$. Further from $\mathcal{X}k^2 > d \ge 2^\delta \mathfrak{p}_1 \cdots \mathfrak{p}_{\omega(d)-\delta'}$, we get

$$k > k_1 := \begin{cases} \sqrt{\frac{2^\delta}{\mathcal{X}} \prod_{i=2}^{\omega(d)+1-\delta'} p_i} & \text{if } 3|d \\ \sqrt{\frac{2^\delta}{\mathcal{X}} \prod_{i=3}^{\omega(d)+2-\delta'} p_i} & \text{if } 3\nmid d. \end{cases}$$

Thus

$$k > k_2 := \max(1733, k_1) \tag{11.2.14}$$

Further we derive from (11.2.13) that

$$\frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_h - 1}{2} < \mathcal{X}_2^h := \begin{cases} \frac{1}{2^{h-1}} \left(\frac{\mathcal{X}k^2}{3\cdot 2^\delta}\right)^{\frac{h-1}{\omega(d)-1-\delta'}} & \text{if } 3|d \\ \frac{1}{2^h} \left(\frac{\mathcal{X}k^2}{2^\delta}\right)^{\frac{h}{\omega(d)-\delta'}} & \text{if } 3\nmid d \end{cases}$$

for $1 \le h \le \omega(d) - \delta'$.

We take $r = [\frac{\omega(d)-1}{2}]$ if d is odd and $r = [\frac{\omega(d)}{2}] - 1$ if d is even. By Corollary 9.3.8 and $|T_1| > .42k$ by Lemma 11.1.3, we have

$$s_{r+1} \ge \frac{.42k}{2^{\omega(d)-r-\theta}} - 2\lambda_r - 2^{r-1}\lambda_1 - \sum_{\mu=2}^{r-1} 2^{r-\mu}\lambda_\mu. \tag{11.2.15}$$

This with Corollary 9.4.4 and $\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_h < \mathcal{X}_1^h$ gives (11.2.13) gives

$$s_{r+1} \ge \mathcal{X}_3 := \begin{cases} \frac{.42k}{2^{\omega(d)-r}} - \frac{\mathcal{X}_1^r}{3\cdot 2^{r-3}} - \sum_{\mu=1}^{r-1} \frac{2^{r+2}}{3} \frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \text{if } 2\nmid d, 3\nmid d \\ \frac{.42k}{2^{\omega(d)-\theta-r}} - \frac{\mathcal{X}_1^r}{3\cdot 2^{r-4+\delta}} - 2^{r-1}(\frac{\mathcal{X}_1}{2^\delta} + 1) - \sum_{\mu=2}^{r-1} \frac{2^{r+3-\delta}}{3} \frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \text{if } 2|d, 3\nmid d \\ \frac{.42k}{2^{\omega(d)-\theta-r}} - \frac{\mathcal{X}_1^r}{9\cdot 2^{r-4+\delta'}} - 2^{r-1}(\frac{\mathcal{X}_1}{3\cdot 2^\delta} + 1) - \sum_{\mu=2}^{r-1} \frac{2^{r+3-\delta'}}{9} \frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \text{if } 3|d, 8\nmid d \\ \frac{.42k}{2^{\omega(d)-r}} - 2(\frac{\mathcal{X}_1^r}{24} + 1) - \sum_{\mu=1}^{r-1} 2^{r-\mu}(\frac{\mathcal{X}_1^\mu}{24} + 1) & \text{if } 8|d, 3|d, r \le 3 \\ \frac{.42k}{2^{\omega(d)-r}} - \frac{\mathcal{X}_1^r}{9\cdot 2^{r-3}} - \sum_{\mu=1}^{3} 2^{r-\mu}(\frac{\mathcal{X}_1^\mu}{24} + 1) - \sum_{\mu=4}^{r-1} \frac{2^{r+2}}{9} \frac{\mathcal{X}_1^\mu}{2^{2\mu}} & \text{if } 8|d, 3|d, r \ge 4. \end{cases}$$

By observing that $\frac{\mathcal{X}_3 - \mathcal{X}_2^r}{k}$ is an increasing function of k and is positive at $k = k_2$ except when $\omega(d) = 7, d$ odd and $3|d$ in which case it is positive at $k = 11500$. Let $k \ge 25500$ when $\omega(d) = 7, d$ odd and $3|d$. Then $s_{r+1} \ge \mathcal{X}_3 > \mathcal{X}_2^r > \frac{\mathfrak{p}_1 - 1}{2} \cdots \frac{\mathfrak{p}_r - 1}{2}$. Therefore by Lemma 9.4.3 with $S = \{A_i : i \in T_{r+1}\}, |S| = s_{r+1}, h = r$ and (11.2.13), we get

$$\mathcal{X}k^3 > n + (k-1)d \ge \mathcal{X}_4 k^2 := \begin{cases} \frac{3}{4} 2^{r+\delta} \mathcal{X}_3 k^2 & \text{if } 3\nmid d \\ \frac{9}{4} 2^{r+\delta-1} \mathcal{X}_3 k^2 & \text{if } 3|d. \end{cases}$$

This is a contradiction by checking that $\frac{\mathcal{X}_4}{k} - \mathcal{X} > 0$ except when d odd, $3|d$ and $\omega(d) = 6, 8, 9$. Thus we may assume that d is odd, $3|d, 6 \le \omega(d) \le 9$ and $k < 25500$ if $\omega(d) = 7$. Also we check that $\frac{\mathcal{X}_4}{k} - \mathcal{X} > 0$ for $k = 5000, 62000, 350000$ according as $\omega(d) = 6, 8, 9$, respectively. Thus we may assume that $k < 5000, 25500, 62000, 350000$ whenever $\omega(d) = 6, 7, 8, 9$, respectively. If $\mathfrak{q}_1 \ge 7$, then we get a contradiction from $d < \mathcal{X}k^2 = \frac{1}{16}k^2$ and $\frac{d}{7\cdot 9\cdot 11\cdot 13\cdot 17\cdot 19} \ge 1, 23, 23\cdot 25, 23\cdot 25\cdot 29$ for $\omega(d) = 6, 7, 8, 9$, respectively. Thus $\mathfrak{q}_1 \in \{3, 5\}$. Further we get $\mathfrak{q}_1 \le 5, \mathfrak{q}_2 \le 7$ if $\omega(d) = 6$, $\mathfrak{q}_1 \le 5, \mathfrak{q}_2 \le 7, \mathfrak{q}_3 \le 11$ if $\omega(d) = 7, 8$ and $\mathfrak{q}_1 = 3, \mathfrak{q}_2 = 5, \mathfrak{q}_3 = 7$ if $\omega(d) = 9$. Thus $\mathfrak{p}_1 = 3$ and $\mathfrak{p}_2 \in \{5, 7\}$ if $\omega(d) = 6$, $\mathfrak{p}_2, \mathfrak{p}_3 \in \{5, 7, 11\}$ if $\omega(d) > 6$. Since $\left(\frac{a_i}{p}\right) = \left(\frac{n}{p}\right)$ for $p|d$, we consider Legendre symbols modulo $3, \mathfrak{q}_1, \mathfrak{q}_2$ to all squarefree positive integers $\le \mathfrak{q}_1$ and $\le \mathfrak{q}_1\mathfrak{q}_2$ to obtain $\lambda_1 \le 1, \lambda_2 \le 3$. Further for $\omega(d) > 6$, we consider Legendre symbols modulo $3, \mathfrak{q}_1, \mathfrak{q}_2$ and $\mathfrak{q}_3$ if $\mathfrak{q}_3 \ne 9$

to all squarefree positive integers $\leq \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ to get $\lambda_3 \leq 17$. Therefore we get from (11.2.15) and Corollary 9.4.4 that

$$s_{r+1} \geq \mathcal{X}_5 := \begin{cases} \frac{.42k}{2^4} - 8 & \text{if } \omega(d) = 6 \\ \frac{.42k}{2^{\omega(d)-3}} - 44 & \text{if } \omega(d) = 7, 8 \\ \frac{.42k}{2^5} - \frac{1}{9}\left(\frac{1}{16}\right)^{\frac{4}{9}} k^{\frac{8}{9}} - 54 & \text{if } \omega(d) = 9. \end{cases}$$

We check that $s_{r+1} \geq \mathcal{X}_5 > \mathcal{X}_2^r > \frac{\mathfrak{p}_1-1}{2} \cdots \frac{\mathfrak{p}_r-1}{2}$ by observing $\frac{\mathcal{X}_5-\mathcal{X}_2^r}{k}$ is an increasing function of k and is positive at k =max$(1733, k_1)$. Therefore by Lemma 9.4.3 with $h = r$ and (11.2.13), we get $\frac{1}{16}k^3 > n + (k-1)d \geq \frac{9}{8}2^r\mathcal{X}_5k^2$. This is a contradiction since $\frac{\mathcal{X}_5}{k} - \frac{1}{18\cdot 2^r} > 0$.

Thus $|S_1| \geq \mathcal{X}_6$ using $|T_1| > .42k$ by Lemma 11.1.3 where $\mathcal{X}_6 = .42k - \mathfrak{h}(3) + 1$ if d is odd and $\mathcal{X}_6 = .42k - \mathfrak{h}(5) + 1$ if d is even. Since there exists a non-degenerate double pair, we apply Lemma 9.3.4 with $z_0 = 2$ to get a partition (d_1, d_2) of d with

$$\begin{cases} \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{[\frac{\omega(d)+1}{2}]} \leq \max(d_1, d_2) < 4k & \text{if } 2 \nmid d \\ \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{[\frac{\omega(d)}{2}]} \leq \max(d_1, d_2) < 4k & \text{if } 2 || d \\ 2\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{[\frac{\omega(d)}{2}]} \leq \max(d_1, d_2) < 8k & \text{if } 4|d. \end{cases}$$

Let $\omega(d) \geq 7 + \delta'$. Then we see from (11.2.12) that $|S_1| \geq \mathcal{X}_6 > \frac{k}{4} > \frac{\mathfrak{p}_1-1}{2} \cdots \frac{\mathfrak{p}_4-1}{2}$. We now apply Lemma 9.4.3 with $h = 4$ to get $\mathcal{X}_0k > n + (k-1)d \geq \frac{3}{4}2^{4+\delta}\mathcal{X}_6k^2 > 3 \cdot 2^\delta k^3$ since $\mathcal{X}_6 > \frac{k}{4}$. This contradicts (11.2.11). Thus $\omega(d) \leq 6 + \delta'$ and $k \geq 1733$ by (11.2.12).

Assume that $k - |R| \geq \mathfrak{h}(3)$. Then from Corollary 9.3.10 with $z_0 = 3$, we get $n + (k-1)d < \mathcal{X}_7k^3$ where $\mathcal{X}_7 = \frac{3}{16}$ if $2||d$ and $\frac{3}{4}$ otherwise. If $2|d$ or $3|d$, then $n + (k-1)d \geq 3(\mathcal{X}_6 - 1)k^2$ if $3|d$ and $n + (k-1)d \geq 2^\delta(\mathcal{X}_6 - 1)k^2$ if $2|d$ contradicting $n + (k-1)d < \mathcal{X}_7k^3$. Thus d is odd, $3 \nmid d$ and $\omega(d) = 5, 6$. By Corollary 9.3.10 with $z_0 = 3$, there is a partition (d_1, d_2) of d with $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \leq$max$(d_1, d_2) < 2(k-1)$. Now we get $\frac{k}{4} > \frac{\mathfrak{p}_1-1}{2}\frac{\mathfrak{p}_2-1}{2}\frac{\mathfrak{p}_3-1}{2}$. Further we check $\mathcal{X}_6 > \frac{k}{4}$ implying $|S_1| \geq \mathcal{X}_6 > \frac{\mathfrak{p}_1-1}{2}\frac{\mathfrak{p}_2-1}{2}\frac{\mathfrak{p}_3-1}{2}$. Therefore we derive from Lemma 9.4.3 with $h = 3$ that $\frac{3}{4}k^3 = \mathcal{X}_7k^3 > n + (k-1)d \geq 6X_6k^2 > \frac{3}{2}k^3$, a contradiction. Hence $k - |R| < \mathfrak{h}(3)$. By Lemma 11.1.2 $(i) - (iv)$, we get d odd, $\omega(d) = 6$ and $1733 \leq k < 2082$. Further from Lemma 11.1.2 $(v), (vi)$, we get $\mathfrak{p}_1 \geq 11$. Now $11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \leq d < 3k^2$ by (11.2.10) and (11.2.11). This is a contradiction. □

COROLLARY 11.2.5. *Equation* (2.1.1) *with* $\omega(d) \geq 5$ *implies that* $k - |R| < 2^{\omega(d)-\theta}$.

PROOF. Assume (2.1.1) with $\omega(d) \geq 5$ and $k - |R| \geq 2^{\omega(d)-\theta}$. By Lemma 9.3.9, there exists a set Ω with at least $2^{\omega(d)-\theta}$ pairs satisfying *Property ND*. Since there are at most $2^{\omega(d)-\theta} - 1$ permissible partitions of d by Lemma 9.3.5 (i), we can find a partition (d_1, d_2) of d and a non-degenerate double pair with respect to (d_1, d_2). This contradicts Lemma 11.2.4. □

LEMMA 11.2.6. *Equation* (2.1.1) *with d odd,* $k \geq 101$ *and* $5 \leq \omega(d) \leq 7$ *implies that* $k - |R| \leq 2^{\omega(d)-1}$.

PROOF. Let d be odd. Assume (2.1.1) with $5 \leq \omega(d) \leq 7$ and $k - |R| \geq 2^{\omega(d)-1} + 1$. By Corollary 11.2.5, we may suppose that $k - |R| < 2^{\omega(d)}$. Further by Lemma 11.1.2 (i), we obtain $k \leq 555, 1056, 2099$ when $\omega(d) = 5, 6, 7$, respectively. Since $k - |R| \geq 2^{\omega(d)-1} + 1$, we derive from Corollary 9.3.11 that there exists a partition (d_1, d_2) of d such that $\mathfrak{D}_{12}$:=max$(d_1, d_2) < (k-1)^2$.

Let $\omega(d) = 5$. Then $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \leq \mathfrak{D}_{12} < (k-1)^2$ implying $\mathfrak{p}_1 \leq 61$ since $67 \cdot 71 \cdot 73 > 555^2$. Also $\mathfrak{p}_2 < \frac{k-1}{\sqrt{\mathfrak{p}_1}}$. By taking $r = 6$ for $208 < k \leq 547$, we get from (9.2.10) and (9.2.14) with $p = \mathfrak{p}_1$ that $k - |R| \geq k - F'(k, r) + \min(-2^{r-2}, \sigma_{61} - 2^{r-1}) \geq 32$ if $k > 208$. Thus $k \leq 208$. Further $\mathfrak{p}_1 \leq 29$ since $31 \cdot 37 \cdot 41 > 208^2$. If $\mathfrak{p}_1 \geq 17$, then we obtain from Lemma 11.1.1 $(a), (b)$ that $207^2 > \mathfrak{D}_{12}$ $\geq$min$(17 \cdot 53 \cdot 59, 23 \cdot 47 \cdot 53)$, a contradiction. Therefore $\mathfrak{p}_1 \leq 13$ and hence $53 \leq \mathfrak{p}_2 < k$ by Lemma 11.1.1 (a). By taking $r = 6$, we get from (9.2.15) with $(p, q) = (\mathfrak{p}_1, \mathfrak{p}_2)$ that $g_{\mathfrak{p}_1,\mathfrak{p}_2} = 2^{r-3}$ if $k \leq 127$ and $g_{\mathfrak{p}_1} = 2^{r-2}$ if $k > 127$ by (9.2.14) with $p = \mathfrak{p}_1$. From (9.2.10) and $\sigma_{\mathfrak{p}_2} \geq 2$, we have

$k-|R| \geq k-F'(k,r)+2-2^{r-3}$ if $k \leq 127$ and $k-|R| \geq k-F'(k,r)+2-2^{r-2}$ if $k > 127$ giving $k-|R| \geq 32$, a contradiction.

Let $\omega(d)=6$. Then $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \leq \mathfrak{D}_{12} < (k-1)^2$ implying $\mathfrak{p}_1 < \mathfrak{p}_2 \leq 97$ since $101 \cdot 103 \cdot 107 > 1055^2$. By taking $r=7$ for $384 < k \leq 1039$, we get from (9.2.10) and (9.2.15) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $k-|R| \geq k-F'(k,r)-2^{r-2} \geq 64$ if $k > 384$. Thus $k \leq 384$. Further $\mathfrak{p}_2 \leq 43$ since $47 \cdot 53 \cdot 59 > 383^2$. Then we derive from Lemma 11.1.1 $(a),(b)$ that $\mathfrak{p}_1=31, \mathfrak{p}_2=41, \mathfrak{p}_3 \geq 47$. Also $k > 319$ since $41 \cdot 47 \cdot 53 > 319^2$. By taking $r=7$ for $319 < k \leq 384$, we obtain from (9.2.10) and (9.2.15) with $(p,q)=(31,41)$ that $k-|R| \geq k-F'(k,r)+\sigma_{31}+\sigma_{41}-2^{r-2} \geq 64$. This is a contradiction.

Let $\omega(d)=7$. Suppose $\mathfrak{p}_1 \leq 19$. By Lemma 11.1.2 $(v),(vi),vii)$, we get $k < 735, 930, 1200$ according as $\mathfrak{p}_1=3, \mathfrak{p}_1 \in \{5,7\}, \mathfrak{p}_1 \geq 11$, respectively. By Lemma 11.1.1 (a), we obtain $\mathfrak{p}_2 \geq 53$. Now $53 \cdot 59 \cdot 61 \leq \frac{\mathfrak{D}_{12}}{\mathfrak{p}_1} < \frac{735^2}{3}, \frac{930^2}{5}, \frac{1200^2}{11}$ according as $\mathfrak{p}_1=3, \mathfrak{p}_1 \in \{5,7\}, \mathfrak{p}_1 \geq 11$, respectively. This is not possible. Thus $\mathfrak{p}_1 \geq 23$. Further $\mathfrak{p}_1 \leq 41, \mathfrak{p}_2 \leq 53$ from $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \leq \mathfrak{D}_{12} < (k-1)^2 \leq 2098^2$. By taking $r=9$, we get from (9.2.10) and (9.2.15) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $k-|R| \geq k-F'(k,r)+\min(-2^{r-3}+\sigma_{53}, -2^{r-2}+\sigma_{41}+\sigma_{53}) \geq 128$ for $k > 1007$. Therefore $k \leq 1007$. Now $1007^2 > \mathfrak{D}_{12} \geq \min(23 \cdot 47 \cdot 53 \cdot 59, 31 \cdot 41 \cdot 47 \cdot 53)$ by Lemma 11.1.1 (b). This is not possible. □

COROLLARY 11.2.7. *Assume* (2.1.1) *with* $\omega(d) \geq 5$. *Then* $k < 308, 556, 1057, 2870$ *and* $2(\omega(d)-\theta)2^{\omega(d)-\theta}$ *for* $\omega(d)=5,6,7,8$ *and* ≥ 9, *respectively. In particular* $k < 2\omega(d)2^{\omega(d)}$.

PROOF. By Corollary 11.2.5 and Lemma 11.2.6, we derive that $k-|R| < 2^{\omega(d)-\theta}$ and $k-|R| \leq 2^{\omega(d)-1}$ if d is odd, $5 \leq \omega(d) \leq 7$. By Lemma 11.1.2 $(i),(ii)$, we get $k < 2(\omega(d)-\theta)2^{\omega(d)-\theta}$ for $\omega(d) \geq 9+\theta$, $k < 4252$ if $\omega(d)=8$ and $k < 308, 556, 1057$ according as $\omega(d)=5,6,7$, respectively. Now it remains to consider $\omega(d)=9$ if $2||d, 4||d$ and $\omega(d)=8$. By Lemma 11.1.2 (ii), it suffices to consider d odd and $\omega(d)=8$. Further $k < 4252$ and $k-|R| < 256$. Suppose $k \geq 2870$. Then $k-|R| \geq 129$ by Lemma 11.1.2 (i) and we derive from Corollary 9.3.11 that there exists a partition (d_1,d_2) of d with $\max(d_1,d_2) < (k-1)^2$. Let $\mathfrak{p}_1 \geq 53$. Then $4252^4 > d \geq 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83$, a contradiction. Thus $\mathfrak{p}_1 \leq 47$. Now we obtain from Lemma 11.1.2 (vi) that $k-|R| \geq 256$, a contradiction. □

LEMMA 11.2.8. (i) *Let d be odd and $\omega(d)=5,6$. Suppose that d is divisible by a prime $\leq k$ when $\omega(d)=5$. Further assume that there exist distinct primes p and q with $pq|d$, $p \leq 19, q \leq k$ when $\omega(d)=6$. Then* (2.1.1) *with $k \geq 101$ has no solution.*
(ii) *Let d be even and $5 \leq \omega(d) \leq 6+\theta$. Assume that $p|d$ with $p \leq 47$ when $\omega(d)=7$. Then* (2.1.1) *with $k \geq 101$ has no solution.*

PROOF. By Lemma 11.2.5, we may suppose that $k-|R| < 2^{\omega(d)-\theta}$.

(i) Let d be odd. From Corollary 11.2.7, we get $k < 308, 556$ when $\omega(d)=5,6$, respectively. Let $\omega(d)=5$. By taking $r=5$ for $101 \leq k < 308$, we get from (9.2.10) and (9.2.14) with $p=\mathfrak{p}_1$ that $k-|R| \geq k-F'(k,r)-2^{r-1} \geq 17$ which is not possible by Lemma 11.2.6.

Let $\omega(d)=6$. Then $53 \leq \mathfrak{p}_2 \leq k$ by Lemma 11.1.1 (a). We take $r=6$. Let $\mathfrak{p}_1 \leq 13$. Then we get from (9.2.15) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $g_{\mathfrak{p}_1,\mathfrak{p}_2}=2^{r-3}$ if $k \leq 127$ and $g_{\mathfrak{p}_1}=2^{r-2}$ if $k > 127$ by (9.2.14) with $p=\mathfrak{p}_1$. From (9.2.10) and $\sigma_{\mathfrak{p}_2} \geq 1$, we have $k-|R| \geq k-F'(k,r)+1-2^{r-3}$ if $k \leq 127$ and $k-|R| \geq k-F'(k,r)+1-2^{r-2}$ if $k > 127$ giving $k-|R| \geq 33$. This contradicts Lemma 11.2.6. Thus $\mathfrak{p}_1 \in \{17,19\}$. We get from (9.2.15) with $(p,q)=(\mathfrak{p}_1,\mathfrak{p}_2)$ that $g_{\mathfrak{p}_1,\mathfrak{p}_2}=2^{r-2}$ if $k \leq 193$ and $g_{\mathfrak{p}_1}=2^{r-1}$ if $k > 193$ by (9.2.14) with $p=\mathfrak{p}_1$. From (9.2.10) and $\sigma_{\mathfrak{p}_1}+\sigma_{\mathfrak{p}_2} \geq \sigma_{19}+1$, we get $k-|R| \geq 33$, a contradiction.

(ii) Let d be even. Then from Lemma 11.1.2 $(ii),(iii),(iv)$, we get $\omega(d)=6, k < 252$ and $\omega(d)=7, k < 430$ if $2||d$; $\omega(d)=6, k < 127$ and $\omega(d)=7, k < 303$ if $4||d$; $\omega(d)=6, k < 220$ if $8|d$. By Lemma 11.1.1, we obtain $\omega(d)=6$, $k < 252$ and $\mathfrak{p}_1 \geq 53$. Further by Lemma 11.1.2, we get $k-|R| \geq 2^{\omega(d)-\theta-1}+1$. This with Corollary 9.3.11 gives $\max(d_1,d_2) < (k-1)^2$ for some partition (d_1,d_2) of d. Since $\max(d_1,d_2) \geq \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \geq 53^3 > 430^2$, we get a contradiction. □

LEMMA 11.2.9. *Equation* (2.1.1) *with $k \geq 101$ implies that $d > 10^{10}$.*

Proof. Assume (2.1.1) with $k \geq 101$ and $d \leq 10^{10}$. By Lemma 11.2.2, we have $\omega(d) \geq 5$. Further we obtain from Corollary 11.2.5 that $k - |R| < 2^{\omega(d)-\theta}$ which we use without reference in the proof.

Let d be odd. Then $\omega(d) \leq 9$ otherwise $d \geq \prod_{i=2}^{11} p_i > 10^{10}$. By Lemma 11.2.8 (i), we see that $d > k^5 > 10^{10}$ if $\omega(d) = 5$. Thus $\omega(d) \geq 6$.

Let $\omega(d) = 6$. If $\mathfrak{p}_1 \leq 19$, then $d > k^5 > 10^{10}$ by Lemma 11.2.8 (i). Therefore $\mathfrak{p}_1 \geq 23$. Also $\mathfrak{p}_1 \leq 37$ otherwise $d \geq 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 > 10^{10}$. Further $k < 556$ by Corollary 11.2.7. Therefore by Lemma 11.1.1 (b), we obtain $d \geq \min(23 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67, 31 \cdot 41 \cdot 47 \cdot 53 \cdot 59 \cdot 61) > 10^{10}$.

Thus $\omega(d) \geq 7$. Then $\mathfrak{p}_1 \leq 13$ otherwise $d \geq \prod_{j=7}^{13} p_i > 10^{10}$. Further $k \geq 1733$ otherwise $d \geq 3 \cdot 53^6 > 10^{10}$ by Lemma 11.1.1 (a). By Corollary 11.2.7, we obtain $\omega(d) \geq 8$.

Let $\omega(d) = 8$. Then $\mathfrak{p}_1 \leq 7$. Now Lemma 11.1.2 $(v), (vi)$ gives $\mathfrak{p}_1 \in \{5, 7\}$. Further $\mathfrak{p}_2 \leq 11$ since $5\prod_{j=6}^{12} p_i > 10^{10}$. This is not possible by Lemma 11.1.2 (vii) since $k \geq 1733$.

Let $\omega(d) = 9$. Then $\mathfrak{p}_1 = 3, \mathfrak{p}_2 = 5$ and $\mathfrak{p}_3 = 7$. This is not possible by Lemma 11.1.2 (vii) since $k \geq 1733$.

Let d be even. Then $\omega(d) \leq 10$ otherwise $d \geq \prod_{i=1}^{11} p_i > 10^{10}$. Further $\omega(d) \leq 9$ for $4|d$ since $4\prod_{i=2}^{10} p_i > 10^{10}$. By Lemma 11.2.8 (ii), we have $\omega(d) \geq 7$. Further $k \geq 1801$ by Lemma 11.1.1 (c) since $2\prod_{i=16}^{21} p_i > 10^{10}$. Now we use Lemma 11.1.2 $(ii), (iii), (iv)$ to obtain either $2||d, \omega(d) = 9, 10$ or $8|d, \omega(d) = 9$.

Let $2||d$. Let $\omega(d) = 9$. Then $\mathfrak{p}_1 \leq 5$ otherwise $d \geq 2\prod_{i=4}^{11} p_i > 10^{10}$. Then $k - |R| \geq 256$ by Lemma 11.1.2 (vii), a contradiction. Let $\omega(d) = 10$. Then $\mathfrak{p}_1 = 3, \mathfrak{p}_2 = 5$ and hence $k - |R| \geq 512$ by Lemma 11.1.2 (vii). This is not possible.

Let $8|d$ and $\omega(d) = 9$. Then $\mathfrak{p}_1 \leq 5$ since $8\prod_{i=4}^{11} p_i > 10^{10}$. By Lemma 11.1.2, we get $k - |R| \geq 512$ which is a contradiction. □

11.3. Proof of Theorem 2.5.2

Suppose that (2.1.1) with $b = 1$ has a solution. By Theorem 2.1.1, Lemmas 11.2.2, 11.2.6 and Corollary 11.2.7, we get $\omega(d) = 5, d$ odd, $k - |R| \leq 16$ and $110 \leq k < 308$. We observe that $\text{ord}_p(a_0 a_1 \cdots a_{k-1})$ is even for each prime p. Therefore the number of i's for which a_i are divisible by p is at most $\sigma'_p = \lceil \frac{k}{p} \rceil$ or $\lceil \frac{k}{p} \rceil - 1$ according as $\lceil \frac{k}{p} \rceil$ is even or odd, respectively. Let $r = 4$. Then from (9.2.3), we get $k - |R| \geq k - F(k, r) - 2^r \geq k - \sum_{p > p_r} \sigma'_p - 2^r$ which is ≥ 17 except at $k = 110, 112, 114, 116, 118, 120, 122, 124$ where $k - |R| \geq 16$. Therefore $k = 110, 112, 114, 116, 118, 120, 122, 124$ and $k - |R| = 16$. Further we may assume that for each prime $11 \leq p \leq k$, there are exactly σ'_p number of i's for which $p|a_i$ and for any i, $pq \nmid a_i$ whenever $11 \leq q \leq k, q \neq p$. By considering the i's for which a_i's are divisible by primes $109, 107$ when $k = 110$; $37, 109, 107$ when $k = 112$; $113, 37, 109, 107$ when $k = 114$; $23, 113, 37, 109, 107$ when $k = 116$; $13, 23, 113, 37, 109, 107$ when $k = 118$; $17, 13, 23, 113, 37, 109, 107$ when $k = 120$; $11, 17, 13, 23, 113, 37, 109, 107$ when $k = 122$ and $41, 11, 17, 13, 23, 113, 37, 109, 107$ when $k = 124$, we get $P(a_{\varsigma_k} a_{\varsigma_k+1} \cdots a_{\varsigma_k+105}) \leq 103$ where $\varsigma_k = 2 + \frac{k-110}{2}$. This is excluded. For instance let $k = 124$. Then $P(a_9 a_{10} \cdots a_{114}) \leq 103$. This gives $103^2 | a_j a_{j+103}$ for $j \in \{9, 10, 11\}$. Let $103^2 | a_9 a_{112}$. Then $101^2 | a_j a_{j+101}$ for $j \in \{10, 12, 13\}$ so that $P(a_{14} a_{15} \cdots a_{110}) \leq 97$. This is excluded by considering by Theorem 10.1.1 with $k = 97$. If $103^2 | a_1 a_{114}$, we obtain similarly that $P(a_{13} a_{14} \cdots a_{109}) \leq 97$ and it is excluded. Thus $103^2 | a_{10} a_{113}$. If $101^2 | a_j a_{j+101}$ for $j \in \{11, 13\}$, we get $P(a_{14} a_{15} \cdots a_{110}) \leq 97$ and is excluded. Hence $101^2 | a_9 a_{110}$ implying $P(a_{11} a_{12} \cdots a_{107}) \leq 97$ and it is excluded again. □

11.4. Proof of Theorem 2.5.3

By Theorem 10.1.1 and Lemmas 11.2.2, 11.2.8 (ii), we may suppose that d is odd, either $\omega(d) = 3, (a_0, a_1, \cdots, a_{k-1}) \in \mathfrak{S}_2$ or $\omega(d) \leq 2, (a_0, a_1, \cdots, a_{k-1}) \in \mathfrak{S}_1 \cup \mathfrak{S}_2$, $(a_0, a_1, \cdots, a_7) \neq (3, 1, 5, 6, 7, 2, 1, 10)$ or its mirror image when $k = 8, \omega(d) = 2$. For $p|d$, we observe from $\left(\frac{q}{p}\right) = 1$ for $q \in \{2, 3, 5, 7\}$ that $p \geq 311$ and therefore $d \geq 311^{\omega(d)}$. Further we observe from Theorem 1.5.1 that (9.3.24) is valid.

Let $\omega(d) = 1$. If $k - |R| \geq 2$, we get $d = d_2 < 4(k-1)$ by Corollary 9.3.10 with $z_0 = 2$, a contradiction since $d \geq 311$. Therefore it remains to consider $k = 8$ and $(a_0, \cdots, a_7) = (3, 1, 5, 6, 7, 2, 1, 10)$ or its mirror image. We exclude the possibility $(a_0, \cdots, a_7) = (3, 1, 5, 6, 7, 2, 1, 10)$ and the proof for excluding its mirror image is similar. We write

$$n = 3x_0^2,\ n + d = x_1^2,\ n + 2d = 5x_2^2,\ n + 3d = 6x_3^2,$$
$$n + 4d = 7x_4^2,\ n + 5d = 2x_5^2,\ n + 6d = x_6^2,\ n + 7d = 10x_7^2.$$

Then we get $5d = x_6^2 - x_1^2 = (x_6 - x_1)(x_6 + x_1)$ implying either $x_6 - x_1 = 1, x_6 + x_1 = 5d$ or $x_6 - x_1 = 5, x_6 + x_1 = d$. We apply Runge's method to arrive at a contradiction. Suppose $x_6 - x_1 = 1, x_6 + x_1 = 5d$. Then $5d = 2x_1 + 1$ and $x_1 \geq 14$. We obtain $(125 \cdot 6x_0x_3x_5)^2 = (25(n+d) - 25d)(25(n+d)+50d)(25(n+d)+100d) = (25x_1^2 - 10x_1 - 5)(25x_1^2 + 20x_1 + 10)(25x_1^2 + 40x_1 + 20) = 15625x_1^6 + 31250x_1^5 + 20625x_1^4 - 3000x_1^3 - 10750x_1^2 - 6000x_1 - 1000 =: \tilde{E}(x_1)$. We see that

$$(125x_1^3 + 125x_1^2 + 20x_1 - 32)^2 > \tilde{E}(x_1) > (125x_1^3 + 125x_1^2 + 20x_1 - 33)^2.$$

This is a contradiction. Let $x_6 - x_1 = 5, x_6 + x_1 = d$. Then we argue as above to conclude that $d = 2x_1 + 5, x_1 \geq 66$ and

$$(x_1^3 + 5x_1^2 + 4x_1 - 32)^2 > \tilde{E}_1(x_1) > (x_1^3 + 5x_1^2 + 4x_1 - 33)^2$$

where $\tilde{E}_1(x_1) = x_1^6 + 10x_1^5 + 33x_1^4 - 24x_1^3 - 430x_1^2 - 1200x_1 - 1000$ is a square. This is again not possible.

Thus $\omega(d) \geq 2$. Let $k \geq 13$ and $(a_0, a_1, \cdots, a_{12}) \neq (3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15)$ or its mirror image when $k = 13$. Let $\mathfrak{g} = 3, 4, 5$ if $k = 13, 14, \geq 19$, respectively. Then from $\nu(1) = 3$ and Lemma 9.3.9, we get a set Ω of pairs (i, j) with $|\Omega| \geq k - |R| + r_3 \geq \mathfrak{g}$ having *Property ND.* Therefore there exists a non-degenerate double pair for $k \geq 14$ when $\omega(d) = 2$. Further there are distinct pairs corresponding to partitions $(d_1, d_2), (d_2, d_1)$ for some divisor d_1 of d for $k \geq 13$ when $\omega(d) = 2$ and for $k \geq 19$ when $\omega(d) = 3$.

Suppose that there is a non-degenerate double pair. Then we get from Lemma 9.3.4 with $z_0 = 2$ that $d < 3k^2 \leq 3 \cdot 24^2$ contradicting $d \geq 311^2$. Thus there is no non-degenerate double pair corresponding to any partition. Again, if there are pairs $(i, j), (g, h)$ corresponding to partitions $(d_1, d_2), (d_2, d_1)$ for some divisor d_1 of d, then we derive from Lemma 9.3.3 that $d < (k-1)^4$. This is not possible since $311^2 \leq d < 12^4$ when $\omega(d) = 2$ and $311^3 \leq d < 23^4$ when $\omega(d) = 3$. Therefore there are no distinct pairs corresponding to partitions $(d_1, d_2), (d_2, d_1)$ for any divisor d_1 of d. Thus it remains to consider $k = 14$ when $\omega(d) = 3$ and either $k = 8, 9$ or $k = 13, (a_0, a_1, \cdots, a_{12}) = (3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15)$ or its mirror image when $\omega(d) = 2$. Also we may suppose that there is a pair (i, j) with $a_i = a_j$ corresponding to the partition $(1, d)$ for each of these possibilities.

Let $k = 8$ and $\omega(d) = 2$. We exclude the possibility $(a_0, a_1, \cdots, a_7) = (2, 3, 1, 5, 6, 7, 2, 1)$ and the proof for excluding its mirror image is similar. We see that either the pair $(0, 6)$ or $(2, 7)$ corresponds to $(1, d)$ and we arrive at a contradiction as in the case $k = 8, \omega(d) = 1$ and $(a_0, \cdots, a_7) = (3, 1, 5, 6, 7, 2, 1, 10)$. Let the pair $(0, 6)$ corresponds to $(1, d)$. Then either $x_6 - x_0 = 1, x_6 + x_0 = 3d$ or $x_6 - x_0 = 3, x_6 + x_0 = d$. Suppose $x_6 - x_0 = 1, x_6 + x_0 = 3d$. Then we obtain $3d = 2x_0 + 1, x_0 \geq 100$ and $(3x_2x_7)^2 = (3n+6d)(3n+21d) = (6x_0^2 + 4x_0 + 2)(6x_0^2 + 14x_0 + 7) = 36x_0^4 + 108x_0^3 + 110x_0^2 + 56x_0 + 14 := \psi_2(x_0)$ is a square. This is a contradiction since $(6x_0^2 + 9x_0 + 3)^2 > \psi_2(x_0) > (6x_0^2 + 9x_0 + 2)^2$. Let $x_6 - x_0 = 3, x_6 + x_0 = d$. Then we argue as above to conclude that $d = 2x_0 + 3, x_0 \geq 100$ and $4x_0^4 + 36x_0^3 + 11x_0^2 + 168x_0 + 126 := \tilde{E}_3(x_0)$ is a square. This is again not possible since $(2x_0^2 + 9x_0 + 8)^2 > \tilde{E}_3(x_0) > (2x_0^2 + 9x_0 + 7)^2$. The other possibility of the pair $(2, 7)$ corresponding to $(1, d)$ is excluded similarly.

Let $k = 9$ and $\omega(d) = 2$. Then (2.1.1) holds with $k = 8$ and $(a_0, \cdots, a_7) = (2, 3, 1, 5, 6, 7, 2, 1)$ or its mirror image. This is already excluded. The case $k = 13, \omega(d) = 2$ and $(a_0, \cdots, a_{12}) = (3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15)$ or its mirror image is excluded as above in the case $k = 8$.

Let $k = 14$ and $\omega(d) = 3$. Let $(a_0, \cdots, a_{13}) = (3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1)$. Then one of the pairs $(0, 9), (1, 6), (1, 13), (6, 13)$ corresponds to the partition $(1, d)$. This is excluded as above in the case $k = 8, \omega(d) = 2$. The proof for excluding the mirror image $(1, 15, 14, 13, 3, 11, 10, 1, 2, 7, 6, 5, 1, 3)$ is similar. □

11.5. Proof of Theorem 2.3.1

Theorem 2.3.1 follow immediately from Theorem 2.5.3 and Lemma 11.2.7. □

11.6. Proof of Theorem 2.4.1

First we show that $d > 10^{10}$. By Lemma 11.2.9 and Theorem 10.1.1, it suffices to consider the case $k = 7$ and $(a_0, a_1, \cdots, a_6)$ given by

$$(2, 3, 1, 5, 6, 7, 2),\ (3, 1, 5, 6, 7, 2, 1),\ (1, 5, 6, 7, 2, 1, 10) \tag{11.6.1}$$

or their mirror images. Then for $p|d$, we have $\left(\frac{q}{p}\right) = 1$ for $q \in \{2, 3, 5, 7\}$. Suppose that $d \le 10^{10}$. Since $\omega(d) \ge 2$, we have $\mathfrak{p}_1 \le 10^5$. For $X > 0$, let

$$\mathcal{P}_0 = \mathcal{P}_0(X) = \{p \le X : \left(\frac{q}{p}\right) = 1,\ q = 2, 3, 5, 7\}.$$

We find that that $\mathcal{P}_0(10^5) = \{311, 479, 719, 839, 1009, \cdots\}$. Thus $\mathfrak{p}_1 \ge 311$ by $\mathfrak{p}_1 \in \mathcal{P}_0(10^5)$. Since $311 \cdot 479 \cdot 719 \cdot 839 > 10^{10}$, we have $\omega(d) \le 3$. Further from $311^2 \cdot 479^2 > 10^{10}$, we get either $\omega(d) = 2, d = \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1^2\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2^2$ or $\omega(d) = 3, d = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Consider $(a_0, a_1, \cdots, a_6) = (2, 3, 1, 5, 6, 7, 2)$. From $d = n + d - n = 3x_1^2 - 2x_0^2$, $3 \nmid x_0$, $4 \nmid x_0x_1$, we get $d \equiv -2 \equiv 1(\text{mod } 3)$ and $d \equiv 3 - 2 \equiv 1(\text{mod } 8)$ giving $d \equiv 1(\text{mod } 24)$. Again from $2(x_6^2 - x_0^2) = n + 6d - n = 6d = 6d_1d_2$, we get $x_6 - x_0 = r_1d_1, x_6 + x_0 = r_2d_2$ with $r_1r_2 = 3$, $r_1d_1 < r_2d_2$ and $(r_1d_1, r_2d_2) \in \mathfrak{D}_3$ with

$$\mathfrak{D}_3 = \begin{cases} \{(1, 3\mathfrak{q}_1\mathfrak{q}_2), (3, \mathfrak{q}_1\mathfrak{q}_2), (\mathfrak{q}_1, 3\mathfrak{q}_2), (3\mathfrak{q}_1, \mathfrak{q}_2), (\mathfrak{q}_2, 3\mathfrak{q}_1)\} & \text{if } \omega(d) = 2 \\ \{(1, 3\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3), (3, \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3), (\mathfrak{p}_1, 3\mathfrak{p}_2\mathfrak{p}_3), (3\mathfrak{p}_1, \mathfrak{p}_2\mathfrak{p}_3), & \\ (\mathfrak{p}_2, 3\mathfrak{p}_1\mathfrak{p}_3), (3\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_3), (\mathfrak{p}_3, 3\mathfrak{p}_1\mathfrak{p}_2), (3\mathfrak{p}_3, \mathfrak{p}_1\mathfrak{p}_2)\} & \text{if } \omega(d) = 3. \end{cases}$$

Then $x_0 = \frac{r_2d_2 - r_1d_1}{2}$ giving $x_2^2 = n + 2d = 2x_0^2 + 2d_1d_2 = \frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 - 2d_1d_2\}$ a square. Now we see from $3x_1^2 = n + d = 2x_0^2 + d = \frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 - 4d_1d_2\}$ that $\frac{1}{6}\{(r_1d_1)^2 + (r_2d_2)^2 - 4d_1d_2\}$ is an square. For each $d = \mathfrak{q}_1\mathfrak{q}_2$, we first check for $d \equiv 1(\text{mod } 24)$ and restrict to such d. Further for each possibility of $(r_1d_1, r_2d_2) \in \mathfrak{D}_3$ with $r_1d_1 < r_2d_2$, we check for $\frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 - 2d_1d_2\}$ being a square and restrict to such pairs (r_1d_1, r_2d_2). Finally we check that $\frac{1}{6}\{(r_1d_1)^2 + (r_2d_2)^2 - 4d_1d_2\}$ is not a square. For example, let $d = 1319 \cdot 4919$. Then $\mathfrak{q}_1 = 1319, \mathfrak{q}_2 = 4919$. We check that $d \equiv 1(\text{mod } 24)$. For each choice $(r_1d_1, r_2d_2) \in \mathfrak{D}_3$ with $r_1d_1 < r_2d_2$, we check for $\frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 - 2d_1d_2\}$ being a square which is possible only for $(r_1d_1, r_2d_2) = (1319, 3 \cdot 4919)$. However we find that $\frac{1}{6}\{(r_1d_1)^2 + (r_2d_2)^2 - 4d_1d_2\}$ is not a square for $(r_1d_1, r_2d_2) = (1319, 3 \cdot 4919)$.

Next we consider $(a_0, a_1, \cdots, a_6) = (3, 1, 5, 6, 7, 2, 1)$. From $d = n + 6d - (n + 5d) = x_6^2 - 2x_5^2$, $3 \nmid x_5, 3|x_6^2$ and $2 \nmid x_6, 4|x_5^2$, we get $d \equiv 1(\text{mod } 24)$. Again from $x_6^2 - x_1^2 = n + 6d - (n + d) = 5d = 5d_1d_2$ we get $x_6 - x_1 = r_1d_1, x_6 + x_1 = r_2d_2$ with $r_1r_2 = 5$, $r_1d_1 < r_2d_2$ and

$$\mathfrak{D}_5 = \begin{cases} \{(1, 5\mathfrak{q}_1\mathfrak{q}_2), (5, \mathfrak{q}_1\mathfrak{q}_2), (\mathfrak{q}_1, 5\mathfrak{q}_2), (5\mathfrak{q}_1, \mathfrak{q}_2), (\mathfrak{q}_2, 5\mathfrak{q}_1)\} & \text{if } \omega(d) = 2 \\ \{(1, 5\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3), (5, \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3), (\mathfrak{p}_1, 5\mathfrak{p}_2\mathfrak{p}_3), (5\mathfrak{p}_1, \mathfrak{p}_2\mathfrak{p}_3), & \\ (\mathfrak{p}_2, 5\mathfrak{p}_1\mathfrak{p}_3), (5\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_3), (\mathfrak{p}_3, 5\mathfrak{p}_1\mathfrak{p}_2), (5\mathfrak{p}_3, \mathfrak{p}_1\mathfrak{p}_2)\} & \text{if } \omega(d) = 3. \end{cases}$$

Thus $x_6 = \frac{r_2d_2 + r_1d_1}{2}$ giving $2x_5^2 = n + 5d = x_6^2 - d = \frac{1}{4}\{(r_1d_1)^2 + (r_2d_2)^2 + 6d\}$ implying $\frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 + 6d\}$ is a square. Further from $7x_4^2 = n + 4d = n + 6d - 2d = x_6^2 - 2d = \frac{1}{4}\{(r_1d_1)^2 + (r_2d_2)^2 + 2d_1d_2\}$, we get $\frac{1}{7}\{(r_1d_1)^2 + (r_2d_2)^2 + 2d_1d_2\}$ is a square. For each $d = \mathfrak{q}_1\mathfrak{q}_2$, we first check for $d \equiv 1(\text{mod } 24)$ and restrict to such d. Further for each possibility of $(r_1d_1, r_2d_2) \in \mathfrak{D}_5$ with $r_1d_1 < r_2d_2$, we check for $\frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 + 6d\}$ being a square and restrict to such pairs (r_1d_1, r_2d_2). Finally we check that $\frac{1}{7}\{(r_1d_1)^2 + (r_2d_2)^2 + 2d\}$ is not a square. Further the case $(a_0, a_1, \cdots, a_6) = (1, 5, 6, 7, 2, 1, 10)$ is excluded by the preceding test.

The case $(a_0, a_1, \cdots, a_6) = (2, 7, 6, 5, 1, 3, 2)$ is similar to $(a_0, a_1, \cdots, a_6) = (2, 3, 1, 5, 6, 7, 2)$ and we obtain $d \equiv -1 (\mathrm{mod}\ 24)$, $\frac{1}{2}\{(r_1d_1)^2 + (r_2d_2)^2 + 2d\}$ and $\frac{1}{6}\{(r_1d_1)^2 + (r_2d_2)^2 + 4d\}$ are squares for each possibility of $(r_1d_1, r_2d_2) \in \mathfrak{D}_3$ with $r_1d_1 < r_2d_2$. This is excluded. The cases $(a_0, a_1, \cdots, a_6) = (1, 2, 7, 6, 5, 1, 3), (10, 1, 2, 7,$
$6, 5, 1)$ are also similar to that of $(a_0, a_1, \cdots, a_6) = (3, 1, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, 1, 10)$ and is excluded. Thus $d > 10^{10}$.

Now we show that $d > k^{\log\log k}$. Since $k^{\log\log k} < 10^{10}$ for $k < 22027$, we may assume that $k \geq 22027$. By Corollary 11.2.7, we obtain $\omega(d) \geq 9$ and $k < 2(\omega(d)-\theta)2^{\omega(d)-\theta} =: \Psi_0(\omega(d)-\theta)$. Further we derive from $22027 \leq k < 2\omega(d)2^{\omega(d)}$ that $\omega(d) \geq 11$. It suffices to show that $\log d > (\log \Psi_0(\omega(d)-\theta))(\log\log \Psi_0(\omega(d)-\theta)) =: \Psi_1(\omega(d)-\theta)$. Let $\Psi_2(l) = l(\log l + \log\log l - 1.076868)$ for $l > 1$. From $d \geq 2^{\delta} \prod_{i=2}^{\omega(d)+1-\delta'} p_i$ and Lemma 3.1.3, we get $\log d > \Psi_2(\omega(d)+1) - \log 2, \Psi_2(\omega(d)) + (\delta - 1)\log 2$ when $2 \nmid d, 2|d$, respectively. It suffices to check for $\omega(d) \geq 11$ that $\Psi_2(\omega(d)+1) - \log 2 - \Psi_1(\omega(d)) > 0$ if $2 \nmid d$, $\Psi_2(\omega(d)) - \Psi_1(\omega(d)-1) > 0$ if $2||d, 4||d$ and $\Psi_2(\omega(d)) + \log 4 - \Psi_1(\omega(d)) > 0$ if $8|d$. This is the case. □

11.7. Proof of Theorem 2.5.1

Suppose Theorem 2.5.1 is not true. Then (2.1.1) is valid with $k \geq 8, b = 1$ and $\omega(d) = 2$ but n and d are not necessarily coprime. Let $n' = \frac{n}{\gcd(n,d)}$ and $d' = \frac{d}{\gcd(n,d)}$. Now, by dividing $\gcd(n, d)^k$ on both sides of (2.1.1), we have

$$n'(n' + d') \cdots (n' + (k-1)d') = \mathfrak{p}_1^{\delta_1}\mathfrak{p}_2^{\delta_2}y_1^2 \tag{11.7.1}$$

where $y_1 > 0$ is an integer and $\delta_1, \delta_2 \in \{0, 1\}$. We may assume that k is odd and $(\delta_1, \delta_2) \neq (0, 0)$ by Theorem 2.5.2 with $\omega(d) = 2$. Let $d' = 1$. Then we see from (1.2.3) for $k \neq 13, 17$ and Corollary 1.2.3 for $k = 13, 17$ that the left hand side of (11.7.1) is divisible by at least three primes $> k$. Therefore there exists a prime p with $p \neq \mathfrak{p}_1, p \neq \mathfrak{p}_2, p > k$ such that it divides a term on the left hand side of (11.7.1) to power at least 2. This implies $n' > k^2$. Now we see from [**47**, Theorem 2] that the left hand side of (11.7.1) is divisible by at least three primes $> k$ to odd powers. This contradicts (11.7.1). Thus $d' > 1$ implying $(\delta_1, \delta_2) \neq (1, 1)$ by $\gcd(n', d') = 1$. Now we may assume that $(\delta_1, \delta_2) = (1, 0)$. Then d' is a power of $\mathfrak{p}_2$. Further we may suppose that $\mathfrak{p}_1 \geq k$ by Theorem 2.5.3. Let $n + i_0d$ with $0 \leq i_0 < k$ be the term divisible by $\mathfrak{p}_1$ on the left hand side of (11.7.1). Then

$$n' \cdots (n' + (i_0 - 1)d')(n' + (i_0 + 1)d') \cdots (n' + (k-1)d') = b'y_2^2$$

where $P(b') < k$ and $y_2 > 0$ is an integer. Now $k = 8$ by [**46**, Theorem 1]. This is not possible since k is odd. □

CHAPTER 12

Equation (2.6.1) with $t \geq k-2$ and $\omega(d)=1$: Proof of Theorem 2.6.2

12.1. Introduction

We shall prove Theorem 2.6.2 in this chapter. From now on, we assume (9.1.1) is valid with $\psi = 2$, $\omega(d) = 1$ and we shall suppose it without reference. Let $d = p^\alpha$. Then $(1, 2)$ is the only partition if $d = 2$ and $(2, 2)$ is the only partition if $d = 4$. For $d \neq 2, 4$, we see that $(\eta, \frac{d}{\eta})$ and $(\frac{d}{\eta}, \eta)$ are the only distinct partitions of d.

In view of Lemma 9.1.1 with $\psi = 2$, there is no loss of generality in assuming that k is prime whenever $k \geq 23$ in the proof of Theorem 2.6.2. Therefore we suppose from now onward without reference that k is prime if $k \geq 23$.

12.2. Lemmas

We apply Theorem 1.4.1 and Lemma 9.4.1 to derive the following result.

Lemma 12.2.1. *Let $k \geq 9$. Then we have*

$$|T_1| > 0.1754k \text{ for } k \geq 81. \tag{12.2.1}$$

and

$$n + \gamma_t d > \eta^2 k^2. \tag{12.2.2}$$

Proof. We observe that $\pi(2k) - \pi(k) > 2$ since $k \geq 9$. Therefore $P(\Delta) > k$ by Theorem 1.4.1. Now we see from (9.1.1) that

$$n + \gamma_t d > k^2. \tag{12.2.3}$$

By (9.4.1), $t \geq k-2$, $\pi_d(k) \leq \pi(k)$ and Lemma 3.1.2 (i), we get

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

Since the right hand side of the above inequality exceeds $0.1754k$ for $k \geq 81$, the assertion (12.2.1) follows.

Now we turn to the proof of (12.2.2). By (12.2.3), it suffices to consider $d = 2^\alpha$ with $\alpha > 1$. From Theorem 1.4.1 and (9.1.1), we have $n + (k-1)d > p^2_{\pi(2k)-2}$. Now we see from (9.4.1) that

$$|T_1| + \pi_d(k) - \pi(2k) > k - 3 - \frac{(k-1)\log(k-1) - (k-3)\log 2 + \log(k-2)}{2\log p_{\pi(2k)-2}} - \pi(2k) \tag{12.2.4}$$

and

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

by Lemma 3.1.2 (i). When $k \geq 60$, we observe that the right hand side of the preceding inequality is positive. Therefore $|T_1| + \pi_d(k) > \pi(2k)$ implying $n + \gamma_t d > 4k^2$ for $k \geq 60$. Thus we may assume $k < 60$. Now we check that the right hand side of (12.2.4) is positive for $k \geq 33$. Therefore we may suppose that $k < 33$ and $n + (k-3)d \leq n + \gamma_t d \leq 4k^2$. Hence $d = 2^\alpha < \frac{4k^2}{k-3}$. For n, d, k satisfying $k < 33, d < \frac{4k^2}{k-3}, n + (k-3)d \leq 4k^2$ and $n + (k-1)d \geq p^2_{\pi(2k)-2}$, we check that there are at least three i with $0 \leq i < k$ such that $n+id$ is divisible by a prime $> k$ to the first power. This is not possible. □

LEMMA 12.2.2. *We have*

$$t - |R| \geq \begin{cases} 5 \text{ for } k \geq 81 \\ 5-\psi \text{ for } k \geq 55 \\ 4-\psi \text{ for } k \geq 28, k \neq 31 \\ 3-\psi \text{ for } k = 31. \end{cases} \tag{12.2.5}$$

PROOF. Suppose $t-|R| < 5$ and $k \geq 292$. Then $|R| \geq 286$ since $t \geq k-2$ and $\prod_{b_i \in R} b_i \geq (1.6)^{|R|}(|R|)!$ by (9.4.9). We observe that (9.3.29) hold for $k \geq 292$ with $i_0 = 0, h_0 = 286$, $z_1 = 1.6, g_1 = 6$, $\mathfrak{m} = 17, \ell = 0, \mathfrak{n}_0 = 1, \mathfrak{n}_1 = 1$ and $\mathfrak{n}_2 = 2^{\frac{1}{6}}$. We check that the right hand side of (9.3.29) is an increasing function of k and it exceeds g_1 at $k = 292$ which is a contradiction. Therefore $t-|R| \geq 5$ for $k \geq 292$. Thus we may assume that $k < 292$. By taking $r = 3$ for $k < 50$, $r = 4$ for $50 \leq k \leq 181$ and $r = 5$ for $181 < k < 292$ in (9.2.3) and (9.2.5), we get $t-|R| \geq k-\psi-F'(k,r)-2^r \geq 7-\psi, 5-\psi, 4-\psi$ for $k \geq 81, 55, 28$, respectively except at $k = 29, 31, 43, 47$ where $t-|R| \geq k-\psi-F(k,r)-2^r \geq k-\psi-F'(k,r)-2^r = 3-\psi$. We may suppose that $k = 29, 43, 47$, $t-|R| = 3-\psi$ and $F(k,r) = F'(k,r)$. Further we may assume that for each prime $7 \leq p \leq k$, there are exactly σ_p number of i's for which $p|b_i$ and for any i, $pq \nmid b_i$ whenever $7 \leq q \leq k, q \neq p$. Now we get a contradiction by considering the i's for which b_i's are divisible by primes $7, 13; 7, 41; 23, 11$ when $k = 29, 43, 47$, respectively. For instance let $k = 29$. Then $7|b_i$ for $i \in \{0, 7, 14, 21, 28\}$. Then $13|b_i$ for $i \in \{h+13j : 0 \leq j \leq 2\}$ with $h = 0, 1, 2$. This is not possible. □

LEMMA 12.2.3. *Let $9 \leq k \leq 23$ and d odd. Suppose that $t-|R| \geq 3$ for $k = 23$ and $t-|R| \geq 2$ for $k < 23$. Then* (9.1.1) *does not hold.*

PROOF. Suppose (9.1.1) holds. From (12.2.2) and Lemma 9.3.5, the partition $(\eta, d\eta^{-1})$ is the only permissible partition for any pair (i,j) with $b_i = b_j$. Let $Q = 2$ if $k = 23$ and $Q = 1$ if $k < 23$. We now apply Lemma 9.3.10 with $z_0 = 3$ for $k = 23$ and $z_0 = 2$ for $k < 23$ to get $d < \frac{4}{Q}(k-1)$, $\theta_1 < \frac{4}{Q(k-1)}$ and

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

Further from (1.4.11), we have $n+(k-1)d \geq n+\gamma_t d \geq p^2_{\pi(2k)-2}$. Therefore $p^\alpha = d < \frac{4}{Q}(k-1)$ and $p^2_{\pi(2k)-2} \leq n+(k-1)d < (k-1)^3\Theta(k-1)$. For these possibilities of n, d and k, we check that there are at least three i with $0 \leq i < k$ such that $n+id$ is divisible by a prime $> k$ to an odd power. This contradicts (9.1.1). □

12.3. Equation (2.6.1) implies $t-|R| \leq 1$

LEMMA 12.3.1. *Equation 9.1.1 with $k \geq 9$ implies that $t-|R| \leq 1$.*

PROOF. Assume that $k \geq 9$ and $t-|R| \geq 2$. Let $d = 2, 4$. Then $|R| \leq t-2$ contradicting $|R| = t$ by (12.2.2) and Lemma 9.3.7. Thus $d \neq 2, 4$. Further by (12.2.2) and Lemma 9.3.7, we have $\nu(b_{i_0}) \leq 2$ and $\nu(B_{i_0}) \leq 2$. Also by Lemma 9.3.5, the partition $(eta, d\eta^{-1})$ is the only permissible partition for any pair (i,j) with $b_i = b_j$.

Let $k \geq 81$. Then $t-|R| \geq 5$ by Lemma 12.2.2. Now we derive from Lemma 9.3.10 with $z_0 = 5$ to get $d < k-1$ giving $\theta_1 \leq \frac{1}{k-1}$ and hence

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

from (9.3.5). On the other hand, we get from (12.2.1) and $\nu(B_{i_0}) \le 2$ that $n+(k-1)d \ge \frac{0.1754k}{2}k^2 \ge 0.1754\frac{k^3}{2}$. Comparing the upper and lower bounds of $n+(k-1)d$, we obtain

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

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

Thus $k < 81$. Let d be even. We see from $\nu(a_i) \le 2$ and (9.2.6) that $\xi_r \le 2g_{2^\delta} \le 2^{r-2}$. Let $r = 3$. From (9.2.1), we get $k-2-F'(k,r) \le \xi_r \le 2^{r-2}$. We find $k-2-F'(k,r) > 2^{r-2}$ by computation. This is a contradiction.

Therefore d is odd. Since $t-|R| \ge 2$, we get from Lemmas 12.2.2 and 9.3.10 with $z_0 = 2,3$ that $d < 2(k-1)$ if $k \ge 55$ and $d < 4(k-1)$ if $k < 55$. Since $g_p(r) \le 2^{r-1}$ for $r = 4, p < 220$ by (9.2.14), we get from (9.2.10) with $r = 4$ that $t-|R| \ge k-2-F'(k,r)-2^{r-1}$ which is ≥ 5 for $k \ge 29$ and ≥ 3 for $k = 23$.

Let $k \ge 29$. Then we get from Lemma 9.3.10 with $z_0 = 5$ that $d < k-1$. By taking $r = 3$ for $k < 53$ and $r = 4$ for $53 \le k < 81$, we derive from (9.2.9), (9.2.14), $\nu(a_i) \le 2$ and (9.2.1) that $k-2-F'(k,r) \le \xi_r \le 2g_p \le 2^r$. We check by computation that $k-2-F'(k,r) > 2^r$. This is a contradiction.

Thus $k \le 23$. Then $t-|R| \ge 3$ for $k = 23$ and $t-|R| \ge 2$ for $k < 23$. By Lemma 12.2.3, this is not possible. □

Corollary 12.3.2. *Let $k \ge 9$. Equation* (9.1.1) *implies that either $k \le 23$ or $k = 31$. Also $P(d) > k$.*

Proof. By Lemmas 12.2.2 and 12.3.1, we see that either $k \le 23$ or $k = 31$. Suppose that $P(d) \le k$. Since $g_{P(d)}(r) \le 2^{r-1}$ for $r = 3$ by (9.2.14), we get from (9.2.10) with $r = 3$ that $t-|R| \ge k-2-F'(k,r)-2^{r-1} \ge 2$ except at $k = 9$ where $t-|R| \ge 1$. This contradicts Lemma 12.3.1 for $k > 9$. Let $k = 9$. By taking $r = 4$, we get from $g_{P(d)}(r) \le 2^{r-2}$ by (9.2.14) and (9.2.10) that $t-|R| \ge k-2-F'(k,4)-2^{4-2} \ge 2$. This contradicts Lemma 12.3.1. □

Corollary 12.3.3. *Let $\psi = 0$. Equation* (9.1.1) *with $P(b) < k$ implies that $k \le 9$.*

Proof. Let $k \ge 10$. By Corollary 12.3.2, we see that either $k \le 23$ or $k = 31$. Let $k = 10$. Then we get from (9.2.5) with $r = 2$ that $t-|R| \ge k-F'(k,r)-2^r = 2$ contradicting Lemma 12.3.1. Thus (2.1.1) does not hold at $k = 10$. By induction, we may assume $k \in \{12, 14, 18, 20\}$ and further there is at most one i for which $p|a_i$ with $p = k-1$. We take $r = 2$ for $k = 12, 14$ and $r = 3$ for $k = 18, 20$. Now we get from $|\{b_i : P(b_i) > p_r\}| \le F'(k,r)-1$ and (9.2.2) that $t-|R| \ge k-F'(k,r)+1-2^r \ge 2$. This contradicts Lemma 12.3.1. □

12.4. Proof of Theorem 2.6.2

Suppose that the assumptions of Theorem 2.6.2 are satisfied and assume (2.1.1) with $\omega(d) = 1$. By Corollary 12.3.2, we have $P(d) > k$ and further we restrict to $k \le 23$ and $k = 31$. Also $t-|R| \le 1$ by Lemma 12.3.1. Further it suffices to prove the assertion for $k \in \{15, 18, 20, 23, 31\}$ since the cases $k = 16, 17$; $k = 19$ and $k = 21, 22$ follows from those of $k = 15, 18$ and 20, respectively.

We shall arrive at a contradiction by showing $t-|R| \ge 2$. For any prime p, let $\sigma'_p = |\{a_i : p|a_i\}|$. Then $\sigma'_p \le \sigma_p$. We use some notation and terminologies as in Section 9.2.

For any subset $\mathcal{I} \subseteq [0,k) \cap \mathbb{Z}$ and primes p_1 and p_2, we have the sets $\mathcal{I}_1$ and $\mathcal{I}_2$ defined in Lemma 10.3.2. Then from $\left(\frac{a_i}{p}\right) = \left(\frac{i-i_p}{p}\right)\left(\frac{d}{p}\right)$, we see that either $\left(\frac{a_i}{p_1}\right) \ne \left(\frac{a_i}{p_2}\right)$ for all $i \in \mathcal{I}_1$ or $\left(\frac{a_i}{p_1}\right) \ne \left(\frac{a_i}{p_2}\right)$ for all $i \in \mathcal{I}_2$. We define $(M, B) = (\mathcal{I}_1, \mathcal{I}_2)$ in the preceding case and $(M, B) = (\mathcal{I}_2, \mathcal{I}_1)$ in the latter case. We call $(\mathcal{I}_1, \mathcal{I}_2, M, B) = (\mathcal{I}_1^k, \mathcal{I}_2^k, M^k, B^k)$ when $\mathcal{I} = [0,k) \cap \mathbb{Z}$. Then for any $\mathcal{I} \subseteq [0,k) \cap \mathbb{Z}$, we have

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

and

$$|M| \geq |M^k| - (k - |\mathcal{I}|), \ |B| \geq |B^k| - (k - |\mathcal{I}|). \tag{12.4.1}$$

12.4.1. The case $k = 15$. Then $\sigma'_7 = 3$ implies that $7|a_{7j}$ for $j = 0, 1, 2$ and $\sigma'_7 \leq 2$ if $7 \nmid a_0a_7a_{14}$. Similarly $\sigma'_{13} = 2$ implies $13|a_0, 13|a_{13}$ or $13|a_1, 13|a_{14}$ and $\sigma'_{13} \leq 1$ otherwise. Thus $|\{a_i : 7|a_i \text{ or } 13|a_i\}| \leq 4$. It suffices to have

$$|\{a_i : p|a_i \text{ for } 5 \leq p \leq 13\}| \leq 7 \tag{12.4.2}$$

since then $t - |R| \geq k - 2 - |\{a_i : p|a_i \text{ for } 5 \leq p \leq 13\}| - 4 \geq 2$ by (9.2.2) with $r = 2$, a contradiction.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. We observe that $P(a_i) \leq 7$ for $i \in \mathcal{M} \cup \mathcal{B}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for a prime $q < k$ other than $5, 11, 13$, we observe that $5|a_i$ whenever $i \in \mathcal{M}$. Since $\sigma_5 \leq 3$ and $|\mathcal{I}| = k - 2$, we obtain from (12.4.1) that $|\mathcal{M}^k| \leq 5$ and $5|a_i$ for at least $|\mathcal{M}^k| - 2$ i's with $i \in \mathcal{M}^k$. Further $5 \nmid a_i$ for $i \in \mathcal{B}$.

By taking the mirror image (9.1.5) of (2.1.1), we may suppose that $0 \leq i_{13} \leq 7$. For each possibility $0 \leq i_{11} < 11$ and $0 \leq i_{13} \leq 7$, we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$ and restrict to those pairs (i_{11}, i_{13}) with $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 5$. We see from $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 6$ that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other. Now we restrict to those pairs (i_{11}, i_{13}) for which there are at most two elements $i \in \mathcal{M}^k$ such that $5 \nmid a_i$. There are 31 such pairs. By counting the multiples of 11 and 13 and also the maximum multiples of 5 in $\mathcal{M}^k$ and the maximum number of multiples of 7 in $\mathcal{B}^k$, we again restrict to those pairs (i_{11}, i_{13}) which do not satisfy (12.4.2). With this procedure, all pairs (i_{11}, i_{13}) are excluded other than

$$(0,6), (1,3), (2,4), (3,5), (4,6), (5,3). \tag{12.4.3}$$

We first explain the procedure by showing how $(i_{11}, i_{13}) = (0, 0)$ is excluded. Now $\mathcal{M}^k = \{5, 10\}$ and $\mathcal{B}^k = \{1, 2, 3, 4, 6, 7, 8, 9, 12, 14\}$. Then there are 3 multiples of 11 and 13, at most 2 multiples of 5 in $\mathcal{M}^k$ and at most 2 multiples of 7 in $\mathcal{B}^k$ implying (12.4.2). Thus $(i_{11}, i_{13}) = (0, 0)$ is excluded.

Let $(i_{11}, i_{13}) = (5, 3)$. Then $\mathcal{M}^k = \{1, 6, 11\}$ and $\mathcal{B}^k = \{0, 2, 4, 7, 8, 9, 10, 12, 13, 14\}$ giving $i_5 = 1$ and $5|a_1a_6a_{11}$. We may assume that $7|a_i$ for $i \in \{0, 7, 14\}$ otherwise (12.4.2) holds. By taking $p_1 = 5, p_2 = 11$ and $\mathcal{I} = \mathcal{B}^k$, we get $\mathcal{I}_1 = \{4, 10, 13\}$ and $\mathcal{I}_2 = \{0, 2, 7, 8, 9, 12, 14\}$. Since $\left(\frac{2}{5}\right) = \left(\frac{2}{11}\right)$, $\left(\frac{7}{5}\right) = \left(\frac{7}{11}\right)$ and $\left(\frac{3}{5}\right) \neq \left(\frac{3}{11}\right)$, we observe that $3|a_i$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$ and $3 \nmid a_i$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$. Thus $a_i \in \{3, 6\}$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$ and $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$. Now from $\left(\frac{a_i}{7}\right) = \left(\frac{i-0}{7}\right)\left(\frac{d}{7}\right)$ and $\left(\frac{3}{7}\right) = \left(\frac{6}{7}\right)$, we see that at least one of $4, 10, 13$ is not in $\mathcal{B}$ implying $i \notin \mathcal{B}$ for at most one $i \in \mathcal{I}_2$. Therefore there are distinct pairs (i_1, i_2) and (j_1, j_2) with $i_1, i_2, j_1, j_2 \in \mathcal{I}_2 \cap \mathcal{B}$ such that $a_{i_1} = a_{i_2}, i_1 > i_2$ and $a_{j_1} = a_{j_2}, j_1 > j_2$ giving $t - |R| \geq 2$. This is a contradiction. Similarly, all other pairs (i_{11}, i_{13}) in (12.4.3) are excluded.

12.4.2. The case $k = 18$. We may assume that $\sigma'_{17} = 1$ and $17 \nmid a_0a_1a_2a_{15}a_{16}a_{17}$ otherwise the assertion follows the case $k = 15$. If $|\{a_i : P(a_i) = 5\}| = 4$, we see from $\{a_i : P(a_i) = 5\} \subseteq \{5, 10, 15, 30\}$ that $a_{i_5}a_{i_5+5}a_{i_5+10}a_{i_5+15} = (150)^2$ implying $(n+i_5d)(n+(i_5+5)d)(n+(i_5+10)d)(n+(i_5+15)d)$ is a square, contradicting Eulers' result for $k = 4$. Thus we have $|\{a_i : P(a_i) = 5\}| \leq 3$. Further for each prime $7 \leq p \leq 13$, we may also assume that $\sigma'_p = \sigma_p$ and for any i, $pq \nmid a_i$ whenever $7 \leq q \leq 17, q \neq p$ otherwise $t - |R| \geq k - 2 - \sum_{7 \leq p \leq 17} \sigma'_p - 3 - 4 \geq 2$ by (9.2.2) with $r = 2$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ and $\left(\frac{17}{11}\right) \neq \left(\frac{17}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q < k, q \neq 5, 17, 11, 13$, we observe that for $i \in \mathcal{M}$, exactly one of $5|a_i$ or $17|a_i$ holds. Thus $5 \cdot 17 \nmid a_i$ whenever $i \in \mathcal{M}$. For $i \in \mathcal{B}$, either $5 \nmid a_i, 17 \nmid a_i$ or $5|a_i, 17|a_i$. Thus for $i \in \mathcal{B}$, we have $P(a_i) \leq 7$ except possibly for one i for which $5 \cdot 17|a_i$. Since $\sigma_5 \leq 4$ and $\sigma'_{17} \leq 1$, we obtain $|\mathcal{M}^k| \leq 7$ and $5|a_i$ for at least $|\mathcal{M}^k| - 3$ i's with $i \in \mathcal{M}^k$. Hence $|\mathcal{M}^k| = 7$ implies that either

$$\{a + 5j : 0 \leq j \leq 3\} \subseteq \mathcal{I}_1^k \text{ or } \{b + 5j : 0 \leq j \leq 3\} \subseteq \mathcal{I}_2^k \tag{12.4.4}$$

for some $a, b \in \{0, 1, 2\}$.

Since $\sigma'_{11} = 2$ and $\sigma'_{13} = 2$, we may suppose that $0 \leq i_{11} \leq 6$ and $0 \leq i_{13} \leq 4$. Further $i_{11} \neq i_{13}$ and $i_{11} + 11 \neq i_{13} + 13$. We observe that either $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 6$ or $|\mathcal{I}_1^k| = |\mathcal{I}_2^k| = 7$. For pairs (i_{11}, i_{13}) with $|\mathcal{I}_1^k| = |\mathcal{I}_2^k| = 7$, we check that (12.4.4) is not valid. Thus we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 6$. There are 16 such pairs. Further we see from $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 8$

that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11}, i_{13}) for which $5|a_i$ for at least 3 elements $i \in \mathcal{M}^k$ otherwise $t - |R| \geq k - 2 - \sum_{7 \leq p \leq 17} \sigma'_p - 2 - 4 \geq 2$ by (9.2.2) with $r = 2$. We find that $(i_{11}, i_{13}) \in \{(1,3), (2,4), (4,0), (5,1)\}$. For these pairs (i_{11}, i_{13}), we check that there are at most 4 multiples a_i of 5 and 17 with $i \in \mathcal{M}^k \cup \mathcal{B}^k$. Thus if $|\{i : i \in \mathcal{B}, 7|a_i\}| \leq 2$, then $t - |R| \geq 2$ by (9.2.2) with $r = 2$. Therefore we may assume that $|\{i : i \in \mathcal{B}, 7|a_i\}| = 3$ and hence $|\{i : i \in \mathcal{B}^k, 7|a_i\}| = 3$. We now restrict to those pairs (i_{11}, i_{13}) for which $|\{i : i \in \mathcal{B}^k, 7|a_i\}| = 3$. They are given by $(i_{11}, i_{13}) \in \{(2,4), (4,0)\}$.

Let $(i_{11}, i_{13}) = (2,4)$. Then by taking $p_1 = 11$ and $p_2 = 13$ as above, we have $\mathcal{M}^k = \{1, 6, 8, 11\}$ and $\mathcal{B}^k = \{0, 3, 5, 7, 9, 10, 12, 14, 15, 16\}$ giving $i_5 = 1$ and $5|a_1 a_6 a_{11}$. We may assume that $17|a_8$ since $17 \nmid a_{16}$. Hence $P(a_i) \leq 7$ for $i \in \mathcal{B}$. Consequently $P(a_i) \leq 7$ for exactly 8 elements $i \in \mathcal{B}^k$ and other 2 elements are not in $\mathcal{B}$. Further $7|a_i$ for $i \in \{0, 7, 14\}$ and $0, 7, 14 \in \mathcal{B}$. Now we take $p_1 = 5, p_2 = 11$ and $\mathcal{I} = \mathcal{B}^k$ to get $\mathcal{I}_1 = \{0, 5, 7, 9\}$ and $\mathcal{I}_2 = \{3, 10, 12, 14, 15\}$. Since $\left(\frac{2}{5}\right) = \left(\frac{2}{11}\right)$, $\left(\frac{7}{5}\right) = \left(\frac{7}{11}\right)$ and $\left(\frac{3}{5}\right) \neq \left(\frac{3}{11}\right)$, we observe that either $3|a_i$ for $i \in \mathcal{I}_1 \cap \mathcal{B}$ or $3|a_i$ for $i \in \mathcal{I}_2 \cap \mathcal{B}$. The former possibility is excluded since $0, 7 \in \mathcal{I}_1 \cap \mathcal{B}$ and the latter is not possible since $14 \in \mathcal{I}_2 \cap \mathcal{B}$. The other case $(i_{11}, i_{13}) = (4, 0)$ is excluded similarly.

12.4.3. The case $k = 20$. We may assume that $\sigma'_{19} = 1$ and $19 \nmid a_0 a_{19}$ otherwise the assertion follows from the case $k = 18$. Also we have $|\{a_i : P(a_i) = 5\}| \leq 3$ by Eulers' result for $k = 4$. Further for each prime $7 \leq p \leq 17$, we may also assume that $\sigma'_p = \sigma_p$ and for any i, $pq \nmid a_i$ whenever $7 \leq p < q \leq 19$ otherwise $t - |R| \geq k - 2 - \sum_{7 \leq p \leq 17} \sigma'_p - 3 - 4 \geq 2$ by (9.2.2) with $r = 2$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. Then as in the case $k = 18$, we observe that for $i \in \mathcal{M}$, exactly one of $5|a_i$ or $17|a_i$ holds but $5 \cdot 17 \nmid a_i$. For $i \in \mathcal{B}$, either $5 \nmid a_i, 17 \nmid a_i$ or $5|a_i, 17|a_i$. Since $\sigma_5 \leq 4$ and $\sigma_{17} \leq 2$, we obtain $|\mathcal{M}^k| \leq 8$ and $5|a_i$ for at least $|\mathcal{M}^k| - 4$ i's with $i \in \mathcal{M}^k$. Hence $|\mathcal{M}^k| = 8$ implies that either

$$\{a + 5j : 0 \leq j \leq 3\} \subseteq \mathcal{I}_1^k \text{ or } \{b + 5j : 0 \leq j \leq 3\} \subseteq \mathcal{I}_2^k \tag{12.4.5}$$

for some $a, b \in \{0, 1, 2, 3, 4\}$.

Since $\sigma'_{11} = 2$ and $\sigma'_{13} = 2$, we may suppose that $0 \leq i_{11} \leq 8$ and $0 \leq i_{13} \leq 6$. Further $i_{11} \neq i_{13}$ and $i_{11} + 11 \neq i_{13} + 13$. We observe that either $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 7$ or $|\mathcal{I}_1^k| = |\mathcal{I}_2^k| = 8$. For pairs (i_{11}, i_{13}) with $|\mathcal{I}_1^k| = |\mathcal{I}_2^k| = 8$, we check that (12.4.5) is not valid. Thus we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 7$. There are 40 such pairs. Further we see from $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 8$ that $\mathcal{M}^k$ is the one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other. Now we restrict to those pairs (i_{11}, i_{13}) for which $5|a_i$ for at least 3 elements $i \in \mathcal{M}^k$ otherwise $t - |R| \geq k - 2 - 1 - \sum_{7 \leq p \leq 17} \sigma'_p - 2 - 4 \geq 2$ by (9.2.2) with $r = 2$. We are left with 22 such pairs. Further by (12.4.1) with $|\mathcal{I}| = k - 2$, we restrict to those pairs (i_{11}, i_{13}) for which there are at least $|\mathcal{M}^k| - 2$ elements $i \in \mathcal{M}^k$ such that $5|a_i$ or $17|a_i$. There are 12 such pairs (i_{11}, i_{13}) and for these pairs, we check that there are at most 4 multiples a_i of 5 and 17 with $i \in \mathcal{M}^k \cup \mathcal{B}^k$. This implies $t - |R| \geq k - 2 - 1 - 4 - \sum_{11 \leq p \leq 13} \sigma'_p - 4 \geq 2$ by (9.2.2) with $r = 2$. For instance, let $(i_{11}, i_{13}) = (3, 5)$. Then $\mathcal{M}^k = \{2, 7, 9, 12\}$ and $\mathcal{B}^k = \{0, 1, 4, 6, 8, 10, 11, 13, 15, 16, 17, 19\}$. Since $5|a_i$ for at least three elements $i \in \mathcal{M}^k$, we get $5|a_i$ for $i \in \{2, 7, 12\}$ giving $i_5 = 2$. Further $17|a_9$ or $5 \cdot 17|a_{17}$ giving 4 multiples a_i of 5 and 17 with $i \in \mathcal{M}^k \cup \mathcal{B}^k$. Thus $t - |R| \geq 2$ as above.

12.4.4. The case $k = 23$. We may assume that $\sigma'_{23} = 1$ and $23 \nmid a_i$ for $0 \leq i \leq 2$ and $20 \leq i < 23$ otherwise the assertion follows from the case $k = 20$. We have $\sigma'_{11} = 3$ if $11|a_{11j}$ with $j = 0, 1, 2$ and $\sigma'_{11} \leq 2$ if $11 \nmid a_0 a_{11} a_{22}$. Also $\sigma'_7 = 4$ implies that $7|a_{7j}$ or $7|a_{1+7j}$ with $0 \leq j \leq 3$ and $\sigma'_7 \leq 3$ otherwise. Thus $|\{a_i : 7|a_i \text{ or } 11|a_i\}| \leq 6$. Further by Eulers result for $k = 4$, we obtain $|\{a_i : P(a_i) = 5\}| \leq 4$. If

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

then we get from (9.2.2) with $r = 2$ that $t - |R| \geq k - 2 - 15 - 4 = 2$, a contradiction. Therefore we have

$$4 + \sum_{7 \leq p \leq 23} \sigma_p - 2 \leq |\{a_i : p|a_i, 5 \leq p \leq 23\}| \leq 4 + \sum_{7 \leq p \leq 19} \sigma_p - 1. \tag{12.4.6}$$

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. Then as in the case $k = 18$, we observe that for $i \in \mathcal{M}$, exactly one of $5|a_i$ or $17|a_i$ holds but $5 \cdot 17 \nmid a_i$. Further for $i \in \mathcal{B}$, either $5 \nmid a_i, 17 \nmid a_i$ or $5 \cdot 17|a_i$. Since $\sigma_5 \leq 5$ and $\sigma_{17} \leq 2$, we obtain $|\mathcal{M}^k| \leq 9$ and $5|a_i$ for at least $|\mathcal{M}^k| - 4$ i's with $i \in \mathcal{M}^k$.

By taking the mirror image (9.1.5) of (2.1.1), we may suppose that $0 \leq i_{11} < 11$ and $0 \leq i_{13} \leq 11$. For each of these pairs (i_{11}, i_{13}), we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$ and check that $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) > 9$. First we restrict to those pairs (i_{11}, i_{13}) for which $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 9$. Therefore $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other set. Now we restrict to those pairs (i_{11}, i_{13}) for which there are at least $|\mathcal{M}^k| - 2$ elements $i \in \mathcal{M}^k$ such that either $5|a_i$ or $17|a_i$. There are 31 such pairs. Next we count the number of multiples of $11, 13$, maximum multiples of $5, 17$ in $\mathcal{M}^k \cup \mathcal{B}^k$ and $7, 19$ in $\mathcal{B}^k$ to check that (12.4.6) is not valid. This is a contradiction. For example, let $(i_{11}, i_{13}) = (0, 2)$. Then $\mathcal{M}^k = \{4, 6, 9, 18, 19, 20\}$ and $\mathcal{B}^k = \{1, 3, 5, 7, 8, 10, 12, 13, 14, 16, 17, 21\}$ giving $5|a_i$ for $i \in \{4, 9, 19\}$, $i_5 = 4$. Further $17|a_i$ for exactly one $i \in \{6, 18, 20\}$ and other two i's in $\{6, 18, 20\}$ deleted. Thus $5 \cdot 17 \nmid a_{14}$ so that (12.4.6) is not valid. For another example, let $(i_{11}, i_{13}) = (4, 0)$. Then $\mathcal{M}^k = \{6, 9, 11, 16, 21\}$ and $\mathcal{B}^k = \{1, 2, 3, 5, 7, 8, 10, 12, 14, 17, 18, 19, 20, 22\}$ giving $5|a_i$ for $i \in \{6, 11, 16, 21\}$, $i_5 = 1$. Further we have either $17|a_9$, $\gcd(5 \cdot 17, a_1) = 1$ or $9 \notin \mathcal{M}, 5 \cdot 17|a_1$. Now $7|a_i$ for at most 3 elements $i \in \mathcal{B}^k$ so that (12.4.6) is not satisfied. This is a contradiction.

12.4.5. The case $k = 31$. From $t - |R| \geq k - 2 - \sum_{7 \leq p \leq 31} \sigma'_p - 8 \geq k - 2 - \sum_{7 \leq p \leq 31} \sigma_p - 8 = 1$ by (9.2.2) and (9.2.5) with $r = 3$, we may assume for each prime $7 \leq p \leq 31$ that $\sigma'_p = \sigma_p$ and for any i, $pq \nmid a_i$ whenever $7 \leq p < q \leq 31$. Let $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. By taking the mirror image (9.1.5) of (2.1.1) and $\sigma_{19} = \sigma_{29} = 2$, we may assume that $i_{29} = 0$ and $1 \leq i_{19} \leq 11, i_{19} \neq 10$. For $p \leq 31$ with $p \neq 19, 29$, since $\left(\frac{p}{19}\right) \neq \left(\frac{p}{29}\right)$ if and only if $p = 11, 13, 17$, we observe that for $i \in \mathcal{M}$, either $11|a_i$ or $13|a_i$ or $17|a_i$. Since $\sigma_{11} + \sigma_{13} + \sigma_{17} \leq 8$, we obtain $|\mathcal{M}^k| \leq 10$ and $p|a_i$ for at least $|\mathcal{M}^k| - 2$ elements $i \in \mathcal{M}^k$ and $p \in \{11, 13, 17\}$. Now for each of the pair (i_{19}, i_{29}) given by $i_{29} = 0, 1 \leq i_{19} \leq 11, i_{19} \neq 10$, we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$. Since $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 14$, we restrict to those pairs (i_{19}, i_{29}) with $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 10$. Then we are left with the only pair $(i_{19}, i_{29}) = (1, 0)$. Further noticing that $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality, we get $\mathcal{M}^k = \{3, 5, 6, 7, 11, 14, 15, 19, 24, 25\}$ and $\mathcal{B}^k = \{2, 4, 8, 9, 10, 12, 13, 16, 17, 18, 21, 22, 23, 26, 27, 28, 30\}$. We find that there are at most 7 elements $i \in \mathcal{M}^k$ for which either $11|a_i$ or $13|a_i$ or $17|a_i$. This is not possible. □

Bibliography

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

[2] E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, J. reine angew. Math. **27** (1844).

[3] Z. Cao, *A note on the Diophantine equation $a^x + b^y = c^z$*, Acta Arith., **91** (1999), 85-93.

[4] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1937), 23-46.

[5] L. E. Dickson, *History of the theory of numbers*, Vol II, Carnegie Institution, Washington, 1920. Reprinted by Chelsea Publishing Company, (1971).

[6] P. Dusart, *Autour de la fonction qui compte le nombre de nombres premiers*, Ph.D thesis, Université de Limoges, (1998).

[7] —, *Inégalitiés explicites pour $\psi(X), \theta(X), \pi(X)$ et les nombres premiers*, C. R. Math. Rep. Acad. Sci. Canada **21(1)**(1999), 53-59, 55.

[8] —, *The kth prime is greater than $k(\log k + \log\log k - 1)$ for $k \geq 2$*, Math. Comp. **68** (1999), no. 225, 411-415.

[9] N. Elkies, *ABC implies Mordell*, Int. Math. Res. Not. **7** (1991).

[10] P. Erdős, *A theorem of Sylvester and Schur*, J. London Math. Soc. **9** (1934), 282-288.

[11] —, *Note on the product of consecutive integers(II)*, J.London Math.Soc. **14** (1939), 245-249.

[12] —, *Note on the product of consecutive integers(III)*, Indag. Math. **17** (1955), 85-90.

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

[14] —, *Some problems on the prime consecutive integers II*, Proc. Wash. State Univ. Conference on Number Theory, Dept. of Math., Washington State Univ., Pullman, Washington, (1971), 13-21.

[15] L. Euler, Mém. Acad. Sc. St. Peters. **8**, 1817-1818 (1780), 3. Comm. Arith., II, 411-413.

[16] M. Faulkner, *On a theorem of Sylvester and Schur*, J. Lond. Math. Soc., **41** (1966), 107-110.

[17] P. Filakovszky and L. Hajdu, *The resolution of the diophantine equation $x(d + d) \cdots (x + (k-1)d) = by^2$ for fixed d*, Acta Arith., **98** (2001), 151-154.

[18] M. Filaseta, C. Finch and J. R. Leidy, *T. N. Shorey's influence in the theory of irreducible polynomials*, Proceedings of the Diophantine Conference in Honor of T. N. Shorey, to appear.

[19] A. Granville and T. J. Tucker, *It's as easy as abc*, Notices of the AMS, **49**, 1224-31.

[20] C. A. Grimm, *A conjecture on consecutive composite numbers*, Amer. Math. monthly, **76** (1969), 1126-1128.

[21] K. Győry, *On the Diophantine equation $n(n+1)\cdots(n+k-1) = bx^l$*, Acta Arith. **83** (1998), 87-92, [Ch 9].

[22] P Hall, *On representatives of subsets*, J. London Math. Soc., **10** (1935), 26-30.

[23] D. Hanson, *On a theorem of Sylvester and Schur*, Canad. Math. Bull., **16** (1973), 195-199.

[24] M. Jutila, *On numbers with a large prime factor II*, J. Indian Math. Soc. (N.S.) **38** (1974), 125-30.

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

[26] S. Laishram, *An estimate for the length of an arithmetic progression the product of whose terms is almost square*, Pub. Math. Debr., **68** (2006), 451-475.

[27] —, *Topics in Diophantine equations*, M.Sc. Thesis, Mumbai University, 2004, online at http://www.math.tifr.res.in/~shanta/MScthesis.pdf.

[28] S. Laishram and T. N. Shorey, *Number of prime divisors in a product of consecutive integers*, Acta Arith. **113** (2004), 327-341.

[29] —, *Number of prime divisors in a product of terms of an arithmetic progression*, Indag. Math., **15(4)** (2004), 505-521.

[30] —, *Greatest prime factor of a product of consecutive integers*, Acta Arith., **120** (2005), 299-306.

[31] —, *Grimm's Conjecture on consecutive integers*, Int. Jour. of Number Theory, **2** (2006), 1-5.

[32] —, *The greatest prime prime divisor of a product of terms in an arithmetic progression*, Indag. Math., **17(3)** (2006), 425-436.

[33] —, *The equation* $n(n+d)\cdots(n+(k-1)d) = by^2$ *with* $\omega(d) \leq 6$ *or* $d \leq 10^{10}$, Acta Arith., accepted for publication.

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

[35] M. Langevin, *Plus grand facteur premier d'entiers consécutifs*, C.r. hebd. Séanc. Acad. Sci., Paris A **280** (1975), 1567-70.

[36] —, *Plus grand facteur premier d'entiers voisins*, C.r. hebd. Séanc. Acad. Sci., Paris A **281** (1975), 491-3.

[37] —, *Méthodes élémentaires en vue du théoremède Sylvester*, Sém. Delange-Pisot-Poitou 1975/76, Exp. G2 pp. 9.

[38] —, *Plus grand facteur premier d'entiers en progression arithḿetique*, Sém. Delange - Pisot - Poitou, 18 eanńee, 1976/77, No.3. pp. 6.

[39] —, *Facteurs premiers d'entiers en progression arithḿetique*, Sém. Delange - Pisot - Poitou, 1977/78, Paris, Exp 4. pp. 7.

[40] R. Marszalek, *On the product of consecutive elements of an arithmetic progression*, Monatsh. für. Math. **100** (1985), 215-222.

[41] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew . Math. **572** (2004), 167-195.

[42] L.J. Mordell, *Diophantine Equations*, Academic Press, London (1969).

[43] P. Moree, *On arithmetical progressions having only few different prime factors in comparison with their length*, Acta Arith. 70 (1995), 295-312.

[44] L. Moser, *Insolvability of* $\binom{2n}{n} = \binom{2a}{a}\binom{2b}{b}$, Canad. Math. Bull.(2), **6** (1963), 167-169.

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

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

[47] —, *Square free part of products of consecutive integers*, Publ. Math. Debrecen, **64** (2004), 79-99.

[48] R. Murty, *Prime Numbers and Marriage*, Appendix 1, The little book of bigger primes by P. Ribenboim, Springer, 269-273.

[49] T. Nagell, *Sur une classe d'équations exponentielles*, Ark. Mat. **3** (1958), 569-582.

[50] R. Obláth, *Über das Produkt funf aufeinander folgender zahlen in einer arithmetischen Reihe,* Publ.Math.Debrecen, **1**, (1950), 222-226.

[51] K. Ramachandra and T. N. Shorey, *On gaps between numbers with a large prime factor*, Acta Arith., **24** (1973), 99-111.

[52] K. Ramachandra, T. N. Shorey and R. Tijdeman, *On Grimm's problem relating to factorisation of a block of consecutive integers*, J. reine angew. Math. **273** (1975), 109-124.

[53] —, *On Grimm's problem relating to factorisation of a block of consecutive integers II*, J. reine angew. Math. **288** (1976), 192-201.

[54] O. Ramaré and R. Rumely, *Primes in Arithmetic Progression*, Math. Comp. 65 (1996), 397-425.

[55] O. Rigge, *On a diophantine problem*, Ark. Mat. Astr. Fys. 27A, **3**, (1940), 10 pp.

[56] G. Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n*, Acta Arith., **42** (1983), 367-389.

[57] H. Robbins, *A remark on stirling's formula*, Amer. Math. Monthly **62**, (1955). 26-29.

[58] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Jour. Math **6** (1962), 64-94.

[59] N. Saradha, *Squares in products with terms in an arithmetic profession*, Acta Arith., **86** (1998), 27-43.

[60] —, *On perfect powers in products with terms from arithmetic progressins*, Acta Arith., **82**, (1997), 147-172.

[61] N. Saradha and T. N. Shorey, *Almost squares and factorisations in consecutive integers*, Compositio Math. **138** (2003), 113-124.

[62] —, *Almost perfect powers in arithmetic progression*, Acta Arith. 99 (2001), 363-388.

[63] —, *Almost squares in arithmetic progression*, Compositio Math. **138** (2003), 73-111.

[64] —, *Contributions towards a conjecture of Erdos on perfect powers in arithmetic progressions*, (to appear).

[65] N. Saradha, T. N. Shorey and R. Tijdeman, *Some extensions and refinements of a theorem of Sylvester*, Acta Arith. **102** (2002), 167-181.

[66] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4**, (1958), 185-208, corrected in Acta Arith. **5**, (1959), 259.

[67] L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, II*, Math. Comp. **30** (1976), 337-360.

[68] I. Schur, *Einige Sätze übner Primzahlen mit Anwendung auf Irreduzibilitätsfragen*, Sitszungsber. Preuss. Akad. Wiss. Phys. Math. Kl., **23**, (1929), 1-24.

[69] I. Schur, *Einige Sätze übner Primzahlen mit Anwendung auf Irreduzibilitätsfragen I*, Sitszungsber. Preuss. Akad. Wiss. Phys. Math. Kl., **14**, (1929), 125-136.

[70] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, J. Reine Angew. Math., **165**, (1931), 52-58.

[71] T. N. Shorey, *On gaps between numbers with a large prime factor II*, Acta Arith., **25** (1974), 365-73.

[72] —, *Exponential diophantine equations involving products of consecutive intergers and related equations*, Number Theory edited by R.P. Bambah, V.C. Dumir and R.J. Hans-Gill, Hindustan Book Agency (1999), 463-495.

[73] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press (1986).

[74] —, *On the number of prime factors of a finite arithmetical progression*, Sichuan Daxue Xuebao **26** (1989), 72-74.

[75] —, *On the greatest prime factor of an arithmetical progression*, A tribute to Paul Erdős, ed. by A. Baker, B. Bollobás and A. Hajnal, Cambridge University Press (1990), 385-389.

[76] —, *Perfect powers in products of terms in an arithmetical progression*, Compositio Math. **75** (1990), 307-344.

[77] J. J. Sylvester, *On arithmetical series*, Messenger of Mathematics, **XXI** (1892), 1-19, 87-120, and Mathematical Papers, **4** (1912), 687-731.

[78] R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), 197-209.

[79] —, *Diophantine equations and diophantine approximations*, Number Theory and Applications, Kluwer Acad. Press, 1989, 215-243.

[80] B. de Weger, *Algorithms for diophantine equations*, Ph.D thesis, CWI, Amsterdam, 1987.